# CCI List
# Version 2014-05-14
# Date 2014-05-14

**CCI:** CCI-000001 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-05-13

**Definition:** The organization develops an access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

**Type:** policy

**Note:** The policy will address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

**Parameter:** Access Control Policy Document

**References:** NIST: NIST SP 800-53 (v3): AC-1 a

NIST: NIST SP 800-53 Revision 4 (v4): AC-1 a 1

NIST: NIST SP 800-53A (v1): AC-1.1 (i and ii)

---

**CCI:** CCI-000004 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-05-13

**Definition:** The organization develops procedures to facilitate the implementation of the access control policy and associated access controls.

**Type:** policy

**Parameter:** Access Control Policy Procedures

**References:** NIST: NIST SP 800-53 (v3): AC-1 b

NIST: NIST SP 800-53 Revision 4 (v4): AC-1 a 2

NIST: NIST SP 800-53A (v1): AC-1.1 (iv and v)

---

**CCI:** CCI-000002 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-14

**Definition:** The organization disseminates the access control policy to organization-defined personnel or roles.

**Type:** policy

**Note:** The policy will address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

**Parameter:** Record of distribution history of access control policy

**References:** NIST: NIST SP 800-53 (v3): AC-1 a

NIST: NIST SP 800-53 Revision 4 (v4): AC-1 a 1

NIST: NIST SP 800-53A (v1): AC-1.1 (iii)

---

**CCI:** CCI-000005 **Status:** draft

**Contributor:** DISA FSO **Published** 2009-09-14

**Date:**

**Definition:** The organization disseminates the procedures to facilitate access control policy and associated access controls to the organization-defined personnel or roles.

**Type:** policy

**Parameter:** Record of distribution history of procedures for implementing access control policy

**References:** NIST: NIST SP 800-53 (v3): AC-1 b<br>
NIST: NIST SP 800-53 Revision 4 (v4): AC-1 a 2<br>
NIST: NIST SP 800-53A (v1): AC-1.1 (vi)

---

**CCI:** CCI-002106 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization documents the access control policy.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-1 a 1

---

**CCI:** CCI-002107 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the personnel or roles to be recipients of the access control policy necessary to facilitate the implementation of the access control policy and associated access controls.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-1 a 1

---

**CCI:** CCI-002108 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the personnel or roles to be recipients of the procedures necessary to facilitate the implementation of the access control policy and associated access controls.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-1 a 1

---

**CCI:** CCI-002109 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization documents procedures to facilitate the implementation of the access control policy and associated access controls.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-1 a 2

---

**CCI:** CCI-001545 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2010-05-11

**Definition:** The organization defines a frequency for reviewing and updating the access control policy.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-1 a

NIST: NIST SP 800-53 Revision 4 (v4): AC-1 b 1

NIST: NIST SP 800-53A (v1): AC-1.2 (i)

---

**CCI:** CCI-001546 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2010-05-11

**Definition:** The organization defines a frequency for reviewing and updating the access control procedures.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-1 b

NIST: NIST SP 800-53 Revision 4 (v4): AC-1 b 2

NIST: NIST SP 800-53A (v1): AC-1.2 (iii)

---

**CCI:** CCI-000003 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-14

**Definition:** The organization reviews and updates the access control policy in accordance with organization-defined frequency.

**Type:** policy

**Note:** The policy will address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

**Parameter:** Document of Review, Comments, and Changes of access control policy

**References:** NIST: NIST SP 800-53 (v3): AC-1 a

NIST: NIST SP 800-53 Revision 4 (v4): AC-1 b 1

NIST: NIST SP 800-53A (v1): AC-1.2 (ii)

---

**CCI:** CCI-000006 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-14

**Definition:** The organization reviews and updates the access control procedures in accordance with organization-defined frequency.

**Type:** policy

**Parameter:** Document of Changes of procedures for implementing access control policy

**References:** NIST: NIST SP 800-53 (v3): AC-1 b

NIST: NIST SP 800-53 Revision 4 (v4): AC-1 b 2

NIST: NIST SP 800-53A (v1): AC-1.2 (iv)

---

**CCI:** CCI-002110 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the information system account types that support the

| | | | |
|---|---|---|---|
| | organizational missions/business functions. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-2 a | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002111 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |
| **Definition:** | The organization identifies and selects the organization-defined information system account types of information system accounts which support organizational missions/business functions. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-2 a | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002112 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |
| **Definition:** | The organization assigns account managers for information system accounts. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-2 b | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000008 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-14 |
| **Definition:** | The organization establishes conditions for group membership. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-2 b<br>NIST: NIST SP 800-53 Revision 4 (v4): AC-2 c<br>NIST: NIST SP 800-53A (v1): AC-2.1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002113 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |
| **Definition:** | The organization establishes conditions for role membership. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-2 c | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002114 | **Status:** | deprecated |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |
| **Definition:** | The organization specifies authorized users of the information system for each account. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-2 d | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002115 | **Status:** | draft |

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization specifies authorized users of the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-2 d

---

**CCI:** CCI-002116 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization specifies authorized group membership on the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-2 d

---

**CCI:** CCI-002117 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization specifies authorized role membership on the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-2 d

---

**CCI:** CCI-002118 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization specifies access authorizations (i.e., privileges) for each account on the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-2 d

---

**CCI:** CCI-002119 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization specifies other attributes for each account on the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-2 d

---

**CCI:** CCI-000010 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-05-13

**Definition:** The organization requires approvals by organization-defined personnel or roles for requests to create information system accounts.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-2 d
NIST: NIST SP 800-53 Revision 4 (v4): AC-2 e
NIST: NIST SP 800-53A (v1): AC-2.1 (i)

---

---

**CCI:** CCI-002120 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the personnel or roles authorized to approve the creation of information system accounts.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-2 e

---

**CCI:** CCI-000011 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-05-13

**Definition:** The organization creates, enables, modifies, disables, and removes information system accounts in accordance with organization-defined procedures or conditions.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-2 e

NIST: NIST SP 800-53 Revision 4 (v4): AC-2 f

NIST: NIST SP 800-53A (v1): AC-2.1 (i)

---

**CCI:** CCI-002121 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the procedures or conditions to be employed when creating, enabling, modifying, disabling, and removing information system accounts.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-2 f

---

**CCI:** CCI-002122 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization monitors the use of information system accounts.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-2 g

---

**CCI:** CCI-002123 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization notifies account managers when accounts are no longer required.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-2 h 1

---

**CCI:** CCI-002124 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization notifies account managers when users are terminated or transferred.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-2 h 2

---

**CCI:** CCI-002125 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization notifies account managers when individual information system usage or need-to-know changes.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-2 h 3

---

**CCI:** CCI-002126 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization authorizes access to the information system based on a valid access authorization.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-2 i 1

---

**CCI:** CCI-002127 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization authorizes access to the information system based on intended system usage.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-2 i 2

---

**CCI:** CCI-002128 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization authorizes access to the information system based on other attributes as required by the organization or associated missions/business functions.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-2 i 3

---

**CCI:** CCI-001547 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2010-05-11

**Definition:** The organization defines the frequency on which it will review information system accounts for compliance with account management requirements.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-2 j
NIST: NIST SP 800-53 Revision 4 (v4): AC-2 j
NIST: NIST SP 800-53A (v1): AC-2.1 (i)

---

**CCI:** CCI-000012

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2009-09-14

**Definition:** The organization reviews information system accounts for compliance with account management requirements per organization-defined frequency.

**Type:** policy

**Note:** Organization-defined frequency

**References:** NIST: NIST SP 800-53 (v3): AC-2 j

NIST: NIST SP 800-53 Revision 4 (v4): AC-2 j

NIST: NIST SP 800-53A (v1): AC-2.1 (i)

---

**CCI:** CCI-002129

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2013-06-24

**Definition:** The organization establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-2 k

---

**CCI:** CCI-000015

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2009-05-13

**Definition:** The organization employs automated mechanisms to support the information system account management functions.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AC-2 (1)

NIST: NIST SP 800-53 Revision 4 (v4): AC-2 (1)

NIST: NIST SP 800-53A (v1): AC-2 (1).1

---

**CCI:** CCI-000016

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2009-05-13

**Definition:** The information system automatically removes or disables temporary accounts after an organization-defined time period for each type of account.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AC-2 (2)

NIST: NIST SP 800-53 Revision 4 (v4): AC-2 (2)

NIST: NIST SP 800-53A (v1): AC-2 (2).1 (ii)

---

**CCI:** CCI-001361

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2009-09-24

**Definition:** The organization defines a time period after which temporary accounts are automatically terminated.

| | | | |
|---|---|---|---|
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-2 (2)<br>NIST: NIST SP 800-53 Revision 4 (v4): AC-2 (2)<br>NIST: NIST SP 800-53A (v1): AC-2 (2).1 (i) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001365 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-24 |
| **Definition:** | The organization defines a time period after which emergency accounts are automatically terminated. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-2 (2)<br>NIST: NIST SP 800-53 Revision 4 (v4): AC-2 (2)<br>NIST: NIST SP 800-53A (v1): AC-2 (2).1 (i) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001682 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2011-05-03 |
| **Definition:** | The information system automatically removes or disables emergency accounts after an organization-defined time period for each type of account. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-2 (2)<br>NIST: NIST SP 800-53 Revision 4 (v4): AC-2 (2)<br>NIST: NIST SP 800-53A (v1): AC-2 (2).1 (ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000017 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-05-13 |
| **Definition:** | The information system automatically disables inactive accounts after an organization-defined time period. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-2 (3)<br>NIST: NIST SP 800-53 Revision 4 (v4): AC-2 (3)<br>NIST: NIST SP 800-53A (v1): AC-2 (3).1 (ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000217 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-24 |
| **Definition:** | The organization defines a time period after which inactive accounts are automatically disabled. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-2 (3)<br>NIST: NIST SP 800-53 Revision 4 (v4): AC-2 (3)<br>NIST: NIST SP 800-53A (v1): AC-2 (3).1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000018 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-05-13 |
| **Definition:** | The information system automatically audits account creation actions. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-2 (4)<br>NIST: NIST SP 800-53 Revision 4 (v4): AC-2 (4)<br>NIST: NIST SP 800-53A (v1): AC-2 (4).1 (i and ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001403 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-24 |
| **Definition:** | The information system automatically audits account modification actions. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-2 (4)<br>NIST: NIST SP 800-53 Revision 4 (v4): AC-2 (4)<br>NIST: NIST SP 800-53A (v1): AC-2 (4).1 (i and ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001404 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-24 |
| **Definition:** | The information system automatically audits account disabling actions. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-2 (4)<br>NIST: NIST SP 800-53 Revision 4 (v4): AC-2 (4)<br>NIST: NIST SP 800-53A (v1): AC-2 (4).1 (i and ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001405 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-24 |
| **Definition:** | The information system automatically audits account removal actions. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-2 (4)<br>NIST: NIST SP 800-53 Revision 4 (v4): AC-2 (4)<br>NIST: NIST SP 800-53A (v1): AC-2 (4).1 (i and ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001683 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2011-05-03 |
| **Definition:** | The information system notifies organization-defined personnel or roles for account creation actions. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-2 (4) | | |

| | | | |
|---|---|---|---|
| | NIST: NIST SP 800-53 Revision 4 (v4): AC-2 (4)<br>NIST: NIST SP 800-53A (v1): AC-2 (4).1 (i and ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001684 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2011-05-03 |
| **Definition:** | The information system notifies organization-defined personnel or roles for account modification actions. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-2 (4)<br>NIST: NIST SP 800-53 Revision 4 (v4): AC-2 (4)<br>NIST: NIST SP 800-53A (v1): AC-2 (4).1 (i and ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001685 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2011-05-03 |
| **Definition:** | The information system notifies organization-defined personnel or roles for account disabling actions. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-2 (4)<br>NIST: NIST SP 800-53 Revision 4 (v4): AC-2 (4)<br>NIST: NIST SP 800-53A (v1): AC-2 (4).1 (i and ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001686 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2011-05-03 |
| **Definition:** | The information system notifies organization-defined personnel or roles for account removal actions. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-2 (4)<br>NIST: NIST SP 800-53 Revision 4 (v4): AC-2 (4)<br>NIST: NIST SP 800-53A (v1): AC-2 (4).1 (i and ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002130 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |
| **Definition:** | The information system automatically audits account enabling actions. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-2 (4) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002131 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |
| **Definition:** | The organization defines the personnel or roles to be notified on account creation, | | |

modification, enabling, disabling, and removal actions.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-2 (4)

---

**CCI:** CCI-002132 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The information system notifies organization-defined personnel or roles for account enabling actions.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-2 (4)

---

**CCI:** CCI-000019 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-14

**Definition:** The organization requires that users log out in accordance with the organization-defined time period of inactivity or description of when to log out.

**Type:** policy

**Note:** Other defined situation could be policy that users must log out at the end of the day.

**References:** NIST: NIST SP 800-53 (v3): AC-2 (5) (a)

NIST: NIST SP 800-53 Revision 4 (v4): AC-2 (5)

NIST: NIST SP 800-53A (v1): AC-2 (5).1 (ii)

---

**CCI:** CCI-001406 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-24

**Definition:** The organization defines a time period of expected inactivity when users are required to log out.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-2 (5) (a)

NIST: NIST SP 800-53 Revision 4 (v4): AC-2 (5)

NIST: NIST SP 800-53A (v1): AC-2 (5).1 (i)

---

**CCI:** CCI-002133 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines other conditions when users are required to log out.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-2 (5)

---

**CCI:** CCI-002134 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines a list of dynamic privilege management capabilities to be

| | | | |
|---|---|---|---|
| | implemented by the information system. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-2 (6) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002135 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |
| **Definition:** | The information system implements the organization-defined list of dynamic privilege management capabilities. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-2 (6) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001407 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-24 |
| **Definition:** | The organization administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-2 (7) (a)<br>NIST: NIST SP 800-53 Revision 4 (v4): AC-2 (7) (a)<br>NIST: NIST SP 800-53A (v1): AC-2 (7).1 (i) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001358 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization establishes privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-2 (7) (a)<br>NIST: NIST SP 800-53 Revision 4 (v4): AC-2 (7) (a)<br>NIST: NIST SP 800-53A (v1): AC-2 (7).1 (i) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001360 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization monitors privileged role assignments. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-2 (7) (b)<br>NIST: NIST SP 800-53 Revision 4 (v4): AC-2 (7) (b)<br>NIST: NIST SP 800-53A (v1): AC-2 (7).1 (ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002136 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |

| | | | |
|---|---|---|---|
| **Definition:** | The organization defines the actions to be taken when privileged role assignments are no longer appropriate. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-2 (7) (c) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002137 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |
| **Definition:** | The organization takes organization-defined actions when privileged role assignments are no longer appropriate. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-2 (7) (c) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002138 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |
| **Definition:** | The organization defines the information system accounts that can be dynamically created. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-2 (8) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002139 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |
| **Definition:** | The information system creates organization-defined information system accounts dynamically. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-2 (8) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002140 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |
| **Definition:** | The organization defines the conditions for establishing shared/group accounts. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-2 (9) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002141 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |
| **Definition:** | The organization only permits the use of shared/group accounts that meet organization-defined conditions for establishing shared/group accounts. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-2 (9) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002142 | **Status:** | draft |

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The information system terminates shared/group account credentials when members leave the group.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-2 (10)

---

**CCI:** CCI-002143 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the circumstances and/or usage conditions that are to be enforced for organization-defined information system accounts.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-2 (11)

---

**CCI:** CCI-002144 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the information system accounts that are to be subject to the enforcement of organization-defined circumstances and/or usage conditions.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-2 (11)

---

**CCI:** CCI-002145 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The information system enforces organization-defined circumstances and/or usage conditions for organization-defined information system accounts.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-2 (11)

---

**CCI:** CCI-002146 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines atypical usage for which the information system accounts are to be monitored.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-2 (12) (a)

---

**CCI:** CCI-002147 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization monitors information system accounts for organization-defined atypical use.

**Type:** policy

|  |  |  |  |
|---|---|---|---|
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-2 (12) (a) | | |

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-002148 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |
| **Definition:** | The organization defines the personnel or roles to whom atypical usage of information system accounts are to be reported. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-2 (12) (b) | | |

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-002149 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |
| **Definition:** | The organization reports atypical usage of information system accounts to organization-defined personnel or roles. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-2 (12) (b) | | |

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-002150 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |
| **Definition:** | The organization defines the time period within which the accounts of users posing a significant risk are to be disabled after discovery of the risk. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-2 (13) | | |

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-002151 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |
| **Definition:** | The organization disables accounts of users posing a significant risk within an organization-defined time period of discovery of the risk. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-2 (13) | | |

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-000213 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-14 |
| **Definition:** | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-3<br>NIST: NIST SP 800-53 Revision 4 (v4): AC-3<br>NIST: NIST SP 800-53A (v1): AC-3.1 | | |

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-000021 | **Status:** | draft |

**Contributor:** DISA FSO **Published Date:** 2009-05-13

**Definition:** The information system enforces dual authorization for organization-defined privileged commands and/or other organization-defined actions.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AC-3 (2)
NIST: NIST SP 800-53 Revision 4 (v4): AC-3 (2)
NIST: NIST SP 800-53A (v1): AC-3 (2).1 (ii)

---

**CCI:** CCI-001408 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-24

**Definition:** The organization defines privileged commands for which dual authorization is to be enforced.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-3 (2)
NIST: NIST SP 800-53 Revision 4 (v4): AC-3 (2)
NIST: NIST SP 800-53A (v1): AC-3

---

**CCI:** CCI-002152 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines other actions necessary for which dual authorization is to be enforced.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-3 (2)

---

**CCI:** CCI-002153 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the mandatory access control policies that are to be enforced over all subjects and objects.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-3 (3)

---

**CCI:** CCI-003014 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-08-30

**Definition:** The information system enforces organization-defined mandatory access control policies over all subjects and objects.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-3 (3)

---

**CCI:** CCI-002154 **Status:** draft

|  |  |  |  |
|---|---|---|---|
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |
| **Definition:** | The mandatory access control policy specifies that the policy is uniformly enforced across all subjects and objects within the boundary of the information system. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-3 (3) (a) | | |

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-002155 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |
| **Definition:** | The mandatory access control policy specifies that a subject that has been granted access to information is constrained from passing the information to unauthorized subjects or objects. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-3 (3) (b) (1) | | |

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-002156 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |
| **Definition:** | The mandatory access control policy specifies that a subject that has been granted access to information is constrained from granting its privileges to other subjects. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-3 (3) (b) (2) | | |

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-002157 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |
| **Definition:** | The mandatory access control policy specifies that a subject that has been granted access to information is constrained from changing one or more security attributes on subjects, objects, the information system, or information system components. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-3 (3) (b) (3) | | |

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-002158 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |
| **Definition:** | The mandatory access control policy specifies that a subject that has been granted access to information is constrained from choosing the security attributes to be associated with newly created or modified objects. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-3 (3) (b) (4) | | |

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-002159 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |

**Definition:** The mandatory access control policy specifies that a subject that has been granted access to information is constrained from choosing the attribute values to be associated with newly created or modified objects.

**Type:** policy

**References:** NIST: [NIST SP 800-53 Revision 4 (v4)](): AC-3 (3) (b) (4)

---

**CCI:** CCI-002160 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The mandatory access control policy specifies that a subject that has been granted access to information is constrained from changing the rules governing access control.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-3 (3) (b) (5)

---

**CCI:** CCI-002161 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines subjects which may explicitly be granted organization-defined privileges such that they are not limited by some or all of the mandatory access control constraints.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-3 (3) (c)

---

**CCI:** CCI-002162 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the privileges that may explicitly be granted to organization-defined subjects such that they are not limited by some or all of the mandatory access control constraints.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-3 (3) (c)

---

**CCI:** CCI-003015 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-08-30

**Definition:** The mandatory access control policy specifies that organization-defined subjects may explicitly be granted organization-defined privileges such that they are not limited by some or all of the mandatory access control constraints.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-3 (3) (c)

---

**CCI:** CCI-002163 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the discretionary access control policies the information system is to enforce over subjects and objects.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-3 (4)

---

**CCI:** CCI-002164 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization specifies in the discretionary access control policies that a subject that has been granted access to information can do one or more of the following: pass the information to any other subjects or objects; grant its privileges to other subjects; change security attributes on subjects, objects, the information system, or the information system's components; choose the security attributes to be associated with newly created or revised objects; and/or change the rules governing access control.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-3 (4)

---

**CCI:** CCI-002165 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The information system enforces organization-defined discretionary access control policies over defined subjects and objects.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-3 (4)

---

**CCI:** CCI-000024 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-14

**Definition:** The information system prevents access to organization-defined security-relevant information except during secure, non-operable system states.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AC-3 (5)
NIST: NIST SP 800-53 Revision 4 (v4): AC-3 (5)
NIST: NIST SP 800-53A (v1): AC-3 (5).1 (ii)

---

**CCI:** CCI-001411 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-24

**Definition:** The organization defines security-relevant information to which the information system prevents access except during secure, non-operable system states.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-3 (5)
NIST: NIST SP 800-53 Revision 4 (v4): AC-3 (5)
NIST: NIST SP 800-53A (v1): AC-3 (5).1 (i)

---

**CCI:** CCI-002166 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the role-based access control policies the information system is to enforce over all subjects and objects.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-3 (7)

---

**CCI:** CCI-002167 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the subjects over which the information system will enforce a role-based access control policy.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-3 (7)

---

**CCI:** CCI-002168 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the objects over which the information system will enforce a role-based access control policy.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-3 (7)

---

**CCI:** CCI-002169 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The information system enforces a role-based access control policy over defined subjects and objects.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-3 (7)

---

**CCI:** CCI-002170 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The information system controls access based upon organization-defined roles and users authorized to assume such roles.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-3 (7)

---

**CCI:** CCI-002171 **Status:** deprecated

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The information system enforces a role-based access control policy over organization-defined subjects.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-3 (7)

---

**CCI:** CCI-002172 **Status:** deprecated
**Contributor:** DISA FSO **Published Date:** 2013-06-24
**Definition:** The information system enforces a role-based access control policy over organization-defined objects.
**Type:** technical
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-3 (7)

---

**CCI:** CCI-002173 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-06-24
**Definition:** The organization defines the roles for which the information system will control access based upon the organization-defined role-based access control policy.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-3 (7)

---

**CCI:** CCI-002174 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-06-24
**Definition:** The organization defines the users for which the information system will control access based upon the organization-defined role-based access control policy.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-3 (7)

---

**CCI:** CCI-002175 **Status:** deprecated
**Contributor:** DISA FSO **Published Date:** 2013-06-24
**Definition:** The information system controls access based upon organization-defined roles authorized to assume such roles, employing the organization-defined role-based access control policy.
**Type:** technical
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-3 (7)

---

**CCI:** CCI-002176 **Status:** deprecated
**Contributor:** DISA FSO **Published Date:** 2013-06-24
**Definition:** The information system controls access based upon organization-defined users authorized to assume such roles, employing the organization-defined role-based access control policy.
**Type:** technical
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-3 (7)

---

**CCI:** CCI-002177 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the rules which will govern the timing of revocation of access authorizations.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-3 (8)

---

**CCI:** CCI-002178 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The information system enforces the revocation of access authorizations resulting from changes to the security attributes of subjects based on organization-defined rules governing the timing of revocations of access authorizations.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-3 (8)

---

**CCI:** CCI-002179 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The information system enforces the revocation of access authorizations resulting from changes to the security attributes of objects based on organization-defined rules governing the timing of revocations of access authorizations.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-3 (8)

---

**CCI:** CCI-002180 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the security safeguards the organization-defined information system or system component is to provide to protect information released outside the established system boundary.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-3 (9) (a)

---

**CCI:** CCI-002181 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines information systems or system components that are to provide organization-defined security safeguards to protect information received outside the established system boundary.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-3 (9) (a)

---

**CCI:** CCI-002182 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The information system does not release information outside of the established system boundary unless the receiving organization-defined information system or system component provides organization-defined security safeguards.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-3 (9) (a)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002183 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |

**Definition:** The organization defines the security safeguards to be used to validate the appropriateness of the information designated for release.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-3 (9) (b)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002184 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |

**Definition:** The information system does not release information outside of the established system boundary unless organization-defined security safeguards are used to validate the appropriateness of the information designated for release.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-3 (9) (b)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002185 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |

**Definition:** The organization defines the conditions on which it will employ an audited override of automated access control mechanisms.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-3 (10)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002186 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |

**Definition:** The organization employs an audited override of automated access control mechanisms under organization-defined conditions.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-3 (10)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001548 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-11 |

**Definition:** The organization defines the information flow control policies for controlling the flow of information within the system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-4

NIST: NIST SP 800-53 Revision 4 (v4): AC-4
NIST: NIST SP 800-53A (v1): AC-4.1 (i)

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-001549 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-11 |
| **Definition:** | The organization defines the information flow control policies for controlling the flow of information between interconnected systems. |  |  |
| **Type:** | policy |  |  |
| **References:** | NIST: NIST SP 800-53 (v3): AC-4<br>NIST: NIST SP 800-53 Revision 4 (v4): AC-4<br>NIST: NIST SP 800-53A (v1): AC-4.1 (i) |  |  |

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-001550 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-11 |
| **Definition:** | The organization defines approved authorizations for controlling the flow of information within the system. |  |  |
| **Type:** | policy |  |  |
| **References:** | NIST: NIST SP 800-53 (v3): AC-4<br>NIST: NIST SP 800-53 Revision 4 (v4): AC-4<br>NIST: NIST SP 800-53A (v1): AC-4.1 (ii) |  |  |

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-001551 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-11 |
| **Definition:** | The organization defines approved authorizations for controlling the flow of information between interconnected systems. |  |  |
| **Type:** | policy |  |  |
| **References:** | NIST: NIST SP 800-53 (v3): AC-4<br>NIST: NIST SP 800-53 Revision 4 (v4): AC-4<br>NIST: NIST SP 800-53A (v1): AC-4.1 (ii) |  |  |

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-001414 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-24 |
| **Definition:** | The information system enforces approved authorizations for controlling the flow of information between interconnected systems based on organization-defined information flow control policies. |  |  |
| **Type:** | technical |  |  |
| **References:** | NIST: NIST SP 800-53 (v3): AC-4<br>NIST: NIST SP 800-53 Revision 4 (v4): AC-4<br>NIST: NIST SP 800-53A (v1): AC-4.1 (iii) |  |  |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001368 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The information system enforces approved authorizations for controlling the flow of information within the system based on organization-defined information flow control policies. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-4<br>NIST: NIST SP 800-53 Revision 4 (v4): AC-4<br>NIST: NIST SP 800-53A (v1): AC-4.1 (iii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002187 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |
| **Definition:** | The organization defines the security attributes to be used to enforce organization-defined information flow control policies. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-4 (1) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002188 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |
| **Definition:** | The organization defines the information, source, and destination objects with which the organization-defined security attributes are to be associated. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-4 (1) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002189 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |
| **Definition:** | The organization defines the information flow control policies to be enforced for flow control decisions. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-4 (1) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002190 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |
| **Definition:** | The information system uses organization-defined security attributes associated with organization-defined information, source, and destination objects to enforce organization-defined information flow control policies as a basis for flow control decisions. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-4 (1) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000026 | **Status:** | draft |

**Contributor:** DISA FSO **Published Date:** 2009-05-13

**Definition:** The information system uses protected processing domains to enforce organization-defined information flow control policies as a basis for flow control decisions.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AC-4 (2)
NIST: NIST SP 800-53 Revision 4 (v4): AC-4 (2)
NIST: NIST SP 800-53A (v1): AC-4 (2).1

---

**CCI:** CCI-002191 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the information flow control policies to be enforced by the information system using protected processing domains.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-4 (2)

---

**CCI:** CCI-000027 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-05-13

**Definition:** The information system enforces dynamic information flow control based on organization-defined policies.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AC-4 (3)
NIST: NIST SP 800-53 Revision 4 (v4): AC-4 (3)
NIST: NIST SP 800-53A (v1): AC-4 (3).1 (ii)

---

**CCI:** CCI-002192 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the policies the information system is to enforce to achieve dynamic information flow control.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-4 (3)

---

**CCI:** CCI-000028 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-05-13

**Definition:** The information system prevents encrypted information from bypassing content-checking mechanisms by employing organization-defined procedures or methods.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-4 (4)
NIST: NIST SP 800-53 Revision 4 (v4): AC-4 (4)
NIST: NIST SP 800-53A (v1): AC-4 (4).1

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002193 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |
| **Definition:** | The organization defines procedures or methods to be employed by the information system to prevent encrypted information from bypassing content-checking mechanisms, such as decrypting the information, blocking the flow of the encrypted information, and/or terminating communications sessions attempting to pass encrypted information. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-4 (4) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000029 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-05-13 |
| **Definition:** | The information system enforces organization-defined limitations on the embedding of data types within other data types. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-4 (5)<br>NIST: NIST SP 800-53 Revision 4 (v4): AC-4 (5)<br>NIST: NIST SP 800-53A (v1): AC-4 (5).1 (ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001415 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-24 |
| **Definition:** | The organization defines limitations for the embedding of data types within other data types. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-4 (5)<br>NIST: NIST SP 800-53 Revision 4 (v4): AC-4 (5)<br>NIST: NIST SP 800-53A (v1): AC-4 (5).1 (i) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000030 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-05-13 |
| **Definition:** | The information system enforces information flow control based on organization-defined metadata. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-4 (6)<br>NIST: NIST SP 800-53 Revision 4 (v4): AC-4 (6)<br>NIST: NIST SP 800-53A (v1): AC-4 (6).1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002194 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |
| **Definition:** | The organization defines the metadata the information system uses to enforce information flow control. | | |

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-4 (6)

---

**CCI:** CCI-000031 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-05-13

**Definition:** The information system enforces organization-defined one-way flows using hardware mechanisms.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AC-4 (7)
NIST: NIST SP 800-53 Revision 4 (v4): AC-4 (7)
NIST: NIST SP 800-53A (v1): AC-4 (7).1 (ii)

---

**CCI:** CCI-001416 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-24

**Definition:** The organization defines one-way information flows to be enforced by the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-4 (7)
NIST: NIST SP 800-53 Revision 4 (v4): AC-4 (7)
NIST: NIST SP 800-53A (v1): AC-4 (7).1 (i)

---

**CCI:** CCI-000032 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-14

**Definition:** The information system enforces information flow control using organization-defined security policy filters as a basis for flow control decisions for organization-defined information flows.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AC-4 (8)
NIST: NIST SP 800-53 Revision 4 (v4): AC-4 (8)
NIST: NIST SP 800-53A (v1): AC-4 (8).1 (ii)

---

**CCI:** CCI-001417 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-24

**Definition:** The organization defines security policy filters to be enforced by the information system and used as a basis for flow control decisions.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-4 (8)
NIST: NIST SP 800-53 Revision 4 (v4): AC-4 (8)
NIST: NIST SP 800-53A (v1): AC-4 (8).1 (i)

---

**CCI:** CCI-002195 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the information flows against which the organization-defined security policy filters are to be enforced.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-4 (8)

---

**CCI:** CCI-002196 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the information flows for which the information system will enforce the use of human reviews under organization-defined conditions.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-4 (9)

---

**CCI:** CCI-002197 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the conditions which will require the use of human reviews of organization-defined information flows.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-4 (9)

---

**CCI:** CCI-002198 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The information system enforces the use of human reviews for organization-defined information flows under organization-defined conditions.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-4 (9)

---

**CCI:** CCI-001553 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2010-05-11

**Definition:** The organization defines the security policy filters that privileged administrators have the capability to enable/disable.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-4 (10)

NIST: NIST SP 800-53 Revision 4 (v4): AC-4 (10)

NIST: NIST SP 800-53A (v1): AC-4 (10).1 (i)

---

**CCI:** CCI-000034 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-05-13

**Definition:** The information system provides the capability for a privileged administrator to enable/disable organization-defined security policy filters under organization-defined conditions.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AC-4 (10)
NIST: NIST SP 800-53 Revision 4 (v4): AC-4 (10)
NIST: NIST SP 800-53A (v1): AC-4 (1).1 (ii)

---

**CCI:** CCI-002199 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the conditions under which the information system provides the capability for privileged administrators to enable/disable organization-defined security policy filters.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-4 (10)

---

**CCI:** CCI-001554 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2010-05-11

**Definition:** The organization defines the security policy filters that privileged administrators have the capability to configure.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-4 (11)
NIST: NIST SP 800-53 Revision 4 (v4): AC-4 (11)
NIST: NIST SP 800-53A (v1): AC-4 (11).1 (i)

---

**CCI:** CCI-000035 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-14

**Definition:** The information system provides the capability for privileged administrators to configure the organization-defined security policy filters to support different security policies.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AC-4 (11)
NIST: NIST SP 800-53 Revision 4 (v4): AC-4 (11)
NIST: NIST SP 800-53A (v1): AC-4 (11).1 (ii)

---

**CCI:** CCI-002200 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the data type identifiers to be used to validate data being transferred between different security domains.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-4 (12)

---

**CCI:** CCI-002201 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The information system, when transferring information between different security domains, uses organization-defined data type identifiers to validate data essential for information flow decisions.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-4 (12)

---

**CCI:** CCI-000219 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-14

**Definition:** The information system, when transferring information between different security domains, decomposes information into organization-defined policy-relevant subcomponents for submission to policy enforcement mechanisms.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AC-4 (13)
NIST: NIST SP 800-53 Revision 4 (v4): AC-4 (13)
NIST: NIST SP 800-53A (v1): AC-4 (13).1

---

**CCI:** CCI-002202 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the policy-relevant subcomponents into which information being transferred between different security domains is to be decomposed for submission to policy enforcement mechanisms.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-4 (13)

---

**CCI:** CCI-001371 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization defines information security policy filters requiring fully enumerated formats which are to be implemented when transferring information between different security domains.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-4 (14)
NIST: NIST SP 800-53 Revision 4 (v4): AC-4 (14)
NIST: NIST SP 800-53A (v1): AC-4 (14).1 (i)

---

**CCI:** CCI-001372 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The information system, when transferring information between different security domains, implements organization-defined security policy filters requiring fully enumerated formats that restrict data structure and content.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AC-4 (14)
NIST: NIST SP 800-53 Revision 4 (v4): AC-4 (14)
NIST: NIST SP 800-53A (v1): AC-4 (14).1 (ii)

---

**CCI:** CCI-001373 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The information system, when transferring information between different security domains, examines the information for the presence of organization-defined unsanctioned information.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AC-4 (15)
NIST: NIST SP 800-53 Revision 4 (v4): AC-4 (15)
NIST: NIST SP 800-53A (v1): AC-4 (15).1 (i)

---

**CCI:** CCI-001374 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The information system, when transferring information between different security domains, prohibits the transfer of organization-defined unsanctioned information in accordance with the organization-defined security policy.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AC-4 (15)
NIST: NIST SP 800-53 Revision 4 (v4): AC-4 (15)
NIST: NIST SP 800-53A (v1): AC-4 (15).1 (ii)

---

**CCI:** CCI-002203 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the unsanctioned information the information system is to examine when transferring information between different security domains.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-4 (15)

---

**CCI:** CCI-002204 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines a security policy which prohibits the transfer of unsanctioned information between different security domains.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-4 (15)

---

**CCI:** CCI-002205 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-06-24
**Definition:** The information system uniquely identifies and authenticates source by organization, system, application, and/or individual for information transfer.
**Type:** technical
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-4 (17)

---

**CCI:** CCI-002206 **Status:** deprecated
**Contributor:** DISA FSO **Published Date:** 2013-06-24
**Definition:** The information system uniquely authenticates source by organization, system, application, and/or individual for information transfer.
**Type:** technical
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-4 (17)

---

**CCI:** CCI-002207 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-06-24
**Definition:** The information system uniquely identifies and authenticates destination by organization, system, application, and/or individual for information transfer.
**Type:** technical
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-4 (17)

---

**CCI:** CCI-002208 **Status:** deprecated
**Contributor:** DISA FSO **Published Date:** 2013-06-24
**Definition:** The information system uniquely authenticates destination by organization, system, application, and/or individual for information transfer.
**Type:** technical
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-4 (17)

---

**CCI:** CCI-002209 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-06-24
**Definition:** The organization defines the techniques to be used to bind security attributes to information.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-4 (18)

---

**CCI:** CCI-002210 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-06-24
**Definition:** The information system binds security attributes to information using organization-defined binding techniques to facilitate information flow policy enforcement.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-4 (18)

---

**CCI:** CCI-002211 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The information system, when transferring information between different security domains, applies the same security policy filtering to metadata as it applies to data payloads.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-4 (19)

---

**CCI:** CCI-002212 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the solutions in approved configurations to be employed to control the flow of organization-defined information across security domains.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-4 (20)

---

**CCI:** CCI-002213 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the information to be subjected to flow control across security domains.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-4 (20)

---

**CCI:** CCI-002214 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization employs organization-defined solutions in approved configurations to control the flow of organization-defined information across security domains.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-4 (20)

---

**CCI:** CCI-002215 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the mechanisms and/or techniques to be used to logically or physically separate information flows.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-4 (21)

---

**CCI:** CCI-002216 **Status:** draft

**Contributor:** DISA FSO **Published** 2013-06-24

**Date:**

**Definition:** The organization defines the types of information required to accomplish logical or physical separation of information flows.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-4 (21)

---

**CCI:** CCI-002217 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The information system separates information flows logically or physically using organization-defined mechanisms and/or techniques to accomplish organization-defined required separations by types of information.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-4 (21)

---

**CCI:** CCI-002218 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The information system provides access from a single device to computing platforms, applications, or data residing on multiple different security domains, while preventing any information flow between the different security domains.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-4 (22)

---

**CCI:** CCI-000036 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-05-19

**Definition:** The organization separates organization-defined duties of individuals.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-5 a<br>
NIST: NIST SP 800-53 Revision 4 (v4): AC-5 a<br>
NIST: NIST SP 800-53A (v1): AC-5.1 (i)

---

**CCI:** CCI-002219 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the duties of individuals that are to be separated.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-5 a

---

**CCI:** CCI-001380 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization documents separation of duties of individuals.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-5 b
NIST: NIST SP 800-53 Revision 4 (v4): AC-5 b
NIST: NIST SP 800-53A (v1): AC-5.1 (ii)

---

**CCI:** CCI-002220 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines information system access authorizations to support separation of duties.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-5 c

---

**CCI:** CCI-000225 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-14

**Definition:** The organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-6
NIST: NIST SP 800-53 Revision 4 (v4): AC-6
NIST: NIST SP 800-53A (v1): AC-6.1

---

**CCI:** CCI-001558 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2010-05-11

**Definition:** The organization defines the security functions (deployed in hardware, software, and firmware) for which access must be explicitly authorized.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-6 (1)
NIST: NIST SP 800-53 Revision 4 (v4): AC-6 (1)
NIST: NIST SP 800-53A (v1): AC-6 (1).1 (i)

---

**CCI:** CCI-002221 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the security-relevant information for which access must be explicitly authorized.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-6 (1)

---

**CCI:** CCI-002222 **Status:** draft

**Contributor:** DISA FSO **Published** 2013-06-24

| | | | |
|---|---|---|---|
| | | **Date:** | |
| **Definition:** | The organization explicitly authorizes access to organization-defined security functions. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-6 (1) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002223 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |
| **Definition:** | The organization explicitly authorizes access to organization-defined security-relevant information. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-6 (1) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000039 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-14 |
| **Definition:** | The organization requires that users of information system accounts or roles, with access to organization-defined security functions or security-relevant information, use non-privileged accounts, or roles, when accessing nonsecurity functions. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-6 (2)<br>NIST: NIST SP 800-53 Revision 4 (v4): AC-6 (2)<br>NIST: NIST SP 800-53A (v1): AC-6 (2).1 (ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001419 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-25 |
| **Definition:** | The organization defines the security functions or security-relevant information to which users of information system accounts, or roles, have access. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-6 (2)<br>NIST: NIST SP 800-53 Revision 4 (v4): AC-6 (2)<br>NIST: NIST SP 800-53A (v1): AC-6 (2).1 (i) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000041 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-05-19 |
| **Definition:** | The organization authorizes network access to organization-defined privileged commands only for organization-defined compelling operational needs. | | |
| **Type:** | policy | | |
| **Note:** | The organization employs the concept of least privilege, limiting authorized access for users (and processes acting on behalf of users) as necessary, to accomplish assigned tasks. | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-6 (3)<br>NIST: NIST SP 800-53 Revision 4 (v4): AC-6 (3) | | |

NIST: NIST SP 800-53A (v1): AC-6 (3).1 (ii)

---

**CCI:** CCI-000042 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-05-19

**Definition:** The organization documents the rationale for authorized network access to organization-defined privileged commands in the security plan for the information system.

**Type:** policy

**Note:** The organization employs the concept of least privilege, limiting authorized access for users (and processes acting on behalf of users) as necessary, to accomplish assigned tasks.

**References:** NIST: NIST SP 800-53 (v3): AC-6 (3)

NIST: NIST SP 800-53 Revision 4 (v4): AC-6 (3)

NIST: NIST SP 800-53A (v1): AC-6 (3).1 (iii)

---

**CCI:** CCI-001420 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-25

**Definition:** The organization defines the privileged commands to which network access is to be authorized only for organization-defined compelling operational needs.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-6 (3)

NIST: NIST SP 800-53 Revision 4 (v4): AC-6 (3)

NIST: NIST SP 800-53A (v1): AC-6 (3).1 (i)

---

**CCI:** CCI-002224 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the compelling operational needs that must be met in order to be authorized network access to organization-defined privileged commands.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-6 (3)

---

**CCI:** CCI-002225 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The information system provides separate processing domains to enable finer-grained allocation of user privileges.

**Type:** policy, technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-6 (4)

---

**CCI:** CCI-002226 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the personnel or roles to whom privileged accounts are to be restricted on the information system.

| | | | |
|---|---|---|---|
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-6 (5) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002227 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |
| **Definition:** | The organization restricts privileged accounts on the information system to organization-defined personnel or roles. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-6 (5) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001422 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-25 |
| **Definition:** | The organization prohibits privileged access to the information system by non-organizational users. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-6 (6)<br>NIST: NIST SP 800-53 Revision 4 (v4): AC-6 (6)<br>NIST: NIST SP 800-53A (v1): AC-6 (6).1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002228 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |
| **Definition:** | The organization defines the frequency on which it conducts reviews of the privileges assigned to organization-defined roles or classes of users. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-6 (7) (a) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002229 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |
| **Definition:** | The organization defines the roles or classes of users that are to have their privileges reviewed on an organization-defined frequency. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-6 (7) (a) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002230 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |
| **Definition:** | The organization reviews the privileges assigned to organization-defined roles or classes of users on an organization-defined frequency to validate the need for such privileges. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-6 (7) (a) | | |

**CCI:** CCI-002231 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-6 (7) (b)

---

**CCI:** CCI-002232 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines software that is restricted from executing at a higher privilege than users executing the software.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-6 (8)

---

**CCI:** CCI-002233 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The information system prevents organization-defined software from executing at higher privilege levels than users executing the software.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-6 (8)

---

**CCI:** CCI-002234 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The information system audits the execution of privileged functions.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-6 (9)

---

**CCI:** CCI-002235 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-6 (10)

---

**CCI:** CCI-000043 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-05-19

**Definition:** The organization defines the maximum number of consecutive invalid logon attempts to the information system by a user during an organization-defined time period.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-7
NIST: NIST SP 800-53 Revision 4 (v4): AC-7
NIST: NIST SP 800-53A (v1): AC-7.1 (i)

---

**CCI:** CCI-001423 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-25

**Definition:** The organization defines the time period in which the organization-defined maximum number of consecutive invalid logon attempts occur.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-7
NIST: NIST SP 800-53 Revision 4 (v4): AC-7
NIST: NIST SP 800-53A (v1): AC-7.1 (i)

---

**CCI:** CCI-000044 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-14

**Definition:** The information system enforces the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AC-7 a
NIST: NIST SP 800-53 Revision 4 (v4): AC-7 a
NIST: NIST SP 800-53A (v1): AC-7.1 (ii)

---

**CCI:** CCI-002236 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the time period the information system will automatically lock the account or node when the maximum number of unsuccessful logon attempts is exceeded.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-7 b

---

**CCI:** CCI-002237 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the delay algorithm to be employed by the information system to delay the next logon prompt when the maximum number of unsuccessful logon attempts is exceeded.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-7 b

---

**CCI:** CCI-002238 **Status:** draft

| | | | |
|---|---|---|---|
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |
| **Definition:** | The information system automatically locks the account or node for either an organization-defined time period, until the locked account or node is released by an administrator, or delays the next logon prompt according to the organization-defined delay algorithm when the maximum number of unsuccessful logon attempts is exceeded. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-7 b | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002239 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |
| **Definition:** | The organization defines the mobile devices that are to be purged/wiped by the information system after an organization-defined number of consecutive, unsuccessful device logon attempts. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-7 (2) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002240 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |
| **Definition:** | The organization defines the purging/wiping requirements/techniques to be used by the information system on organization-defined mobile devices after an organization-defined number of consecutive, unsuccessful device logon attempts. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-7 (2) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002241 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |
| **Definition:** | The organization defines the number of consecutive, unsuccessful device logon attempts after which the information system will purge/wipe organization-defined mobile devices. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-7 (2) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002242 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |
| **Definition:** | The information system purges/wipes information from organization-defined mobile devices based on organization-defined purging/wiping requirements/techniques after an organization-defined number of consecutive, unsuccessful device logon attempts. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-7 (2) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000048 | **Status:** | draft |

**Contributor:** DISA FSO **Published Date:** 2009-05-19

**Definition:** The information system displays an organization-defined system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AC-8 a<br>
NIST: NIST SP 800-53 Revision 4 (v4): AC-8 a<br>
NIST: NIST SP 800-53A (v1): AC-8.1 (ii)

---

**CCI:** CCI-002243 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization-defined information system use notification message or banner is to state that users are accessing a U.S. Government information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-8 a 1

---

**CCI:** CCI-002244 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization-defined information system use notification message or banner is to state that information system usage may be monitored, recorded, and subject to audit.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-8 a 2

---

**CCI:** CCI-002245 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization-defined information system use notification message or banner is to state that unauthorized use of the information system is prohibited and subject to criminal and civil penalties.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-8 a 3

---

**CCI:** CCI-002246 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization-defined information system use notification message or banner is to state that use of the information system indicates consent to monitoring and recording.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-8 a 4

---

**CCI:** CCI-002247 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the use notification message or banner the information system displays to users before granting access to the system.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-8 a

---

**CCI:** CCI-000050 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-14

**Definition:** The information system retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AC-8 b
NIST: NIST SP 800-53 Revision 4 (v4): AC-8 b
NIST: NIST SP 800-53A (v1): AC-8.1 (iii)

---

**CCI:** CCI-001384 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The information system, for publicly accessible systems, displays system use information organization-defined conditions before granting further access.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AC-8 c
NIST: NIST SP 800-53 Revision 4 (v4): AC-8 c 1
NIST: NIST SP 800-53A (v1): AC-8.2 (i)

---

**CCI:** CCI-001385 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The information system, for publicly accessible systems, displays references, if any, to monitoring that are consistent with privacy accommodations for such systems that generally prohibit those activities.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AC-8 c
NIST: NIST SP 800-53 Revision 4 (v4): AC-8 c 2
NIST: NIST SP 800-53A (v1): AC-8.2 (ii)

---

**CCI:** CCI-001386 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The information system, for publicly accessible systems, displays references, if any, to recording that are consistent with privacy accommodations for such systems that generally prohibit those activities.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AC-8 c
NIST: NIST SP 800-53 Revision 4 (v4): AC-8 c 2
NIST: NIST SP 800-53A (v1): AC-8.2 (ii)

---

**CCI:** CCI-001387 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The information system, for publicly accessible systems, displays references, if any, to auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AC-8 c
NIST: NIST SP 800-53 Revision 4 (v4): AC-8 c 2
NIST: NIST SP 800-53A (v1): AC-8.2 (ii)

---

**CCI:** CCI-001388 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The information system, for publicly accessible systems, includes a description of the authorized uses of the system.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AC-8 c
NIST: NIST SP 800-53 Revision 4 (v4): AC-8 c 3
NIST: NIST SP 800-53A (v1): AC-8.2 (iii)

---

**CCI:** CCI-002248 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the conditions of use which are to be displayed to users of the information system before granting further access.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-8 c 1

---

**CCI:** CCI-000052 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-14

**Definition:** The information system notifies the user, upon successful logon (access) to the system, of the date and time of the last logon (access).

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AC-9
NIST: NIST SP 800-53 Revision 4 (v4): AC-9
NIST: NIST SP 800-53A (v1): AC-9.1

---

**CCI:** CCI-000053 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-14
**Definition:** The information system notifies the user, upon successful logon/access, of the number of unsuccessful logon/access attempts since the last successful logon/access.
**Type:** technical
**References:** NIST: NIST SP 800-53 (v3): AC-9 (1)
NIST: NIST SP 800-53 Revision 4 (v4): AC-9 (1)
NIST: NIST SP 800-53A (v1): AC-9 (1).1

---

**CCI:** CCI-001389 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-22
**Definition:** The organization defines the time period that the information system notifies the user of the number of successful logon/access attempts.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): AC-9 (2)
NIST: NIST SP 800-53 Revision 4 (v4): AC-9 (2)
NIST: NIST SP 800-53A (v1): AC-9 (2).1 (i)

---

**CCI:** CCI-001390 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-22
**Definition:** The organization defines the time period that the information system notifies the user of the number of unsuccessful logon/access attempts.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): AC-9 (2)
NIST: NIST SP 800-53 Revision 4 (v4): AC-9 (2)
NIST: NIST SP 800-53A (v1): AC-9 (2).1 (i)

---

**CCI:** CCI-001391 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-22
**Definition:** The information system notifies the user of the number of successful logins/accesses that occur during the organization-defined time period.
**Type:** technical
**References:** NIST: NIST SP 800-53 (v3): AC-9 (2)
NIST: NIST SP 800-53 Revision 4 (v4): AC-9 (2)
NIST: NIST SP 800-53A (v1): AC-9 (2).1 (ii)

---

**CCI:** CCI-001392 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-22
**Definition:** The information system notifies the user of the number of unsuccessful login/access

attempts that occur during organization-defined time period.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AC-9 (2)
NIST: NIST SP 800-53 Revision 4 (v4): AC-9 (2)
NIST: NIST SP 800-53A (v1): AC-9 (2).1 (ii)

---

**CCI:** CCI-001393 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization defines the security-related characteristics/parameters of the user's account which, when changed, will result in a notification being provided to the user during the organization-defined time period.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-9 (3)
NIST: NIST SP 800-53 Revision 4 (v4): AC-9 (3)
NIST: NIST SP 800-53A (v1): AC-9 (3).1 (ii)

---

**CCI:** CCI-001394 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization defines the time period during which organization-defined security-related changes to the user's account are to be tracked.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-9 (3)
NIST: NIST SP 800-53 Revision 4 (v4): AC-9 (3)
NIST: NIST SP 800-53A (v1): AC-9 (3).1 (i)

---

**CCI:** CCI-001395 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The information system notifies the user of changes to organization-defined security-related characteristics/parameters of the user's account that occur during the organization-defined time period.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AC-9 (3)
NIST: NIST SP 800-53 Revision 4 (v4): AC-9 (3)
NIST: NIST SP 800-53A (v1): AC-9 (3).1 (ii)

---

**CCI:** CCI-002249 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the information, in addition to the date and time of the last logon (access), to be included in the notification to the user upon successful logon (access).

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-9 (4)

---

**CCI:** CCI-002250 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The information system notifies the user, upon successful logon (access), of the organization-defined information to be included in addition to the date and time of the last logon (access).

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-9 (4)

---

**CCI:** CCI-002251 **Status:** deprecated

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The information system notifies the user, upon successful logon (access), of the date and time of the last logon (access).

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-9 (4)

---

**CCI:** CCI-000054 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-05-19

**Definition:** The information system limits the number of concurrent sessions for each organization-defined account and/or account type to an organization-defined number of sessions.

**Type:** technical

**Note:** The organization may define the maximum number of concurrent sessions for an information system account globally, by account type, by account, or a combination. This control addresses concurrent sessions for a given information system account and does not address concurrent sessions by a single user via multiple system accounts.

**References:** NIST: NIST SP 800-53 (v3): AC-10
NIST: NIST SP 800-53 Revision 4 (v4): AC-10
NIST: NIST SP 800-53A (v1): AC-10.1 (ii)

---

**CCI:** CCI-000055 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-05-19

**Definition:** The organization defines the maximum number of concurrent sessions to be allowed for each organization-defined account and/or account type.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-10
NIST: NIST SP 800-53 Revision 4 (v4): AC-10
NIST: NIST SP 800-53A (v1): AC-10.1 (i)

---

**CCI:** CCI-002252 **Status:** draft

**Contributor:** DISA FSO **Published** 2013-06-24

**Date:**

**Definition:** The organization defines the accounts and/or account types for which the information system will limit the number of concurrent sessions.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-10

---

**CCI:** CCI-002253 **Status:** deprecated

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the account types for which the information system will limit the number of concurrent sessions.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-10

---

**CCI:** CCI-000057 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-05-19

**Definition:** The information system initiates a session lock after the organization-defined time period of inactivity.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AC-11 a

NIST: NIST SP 800-53 Revision 4 (v4): AC-11 a

NIST: NIST SP 800-53A (v1): AC-11.1 (ii)

---

**CCI:** CCI-000058 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-05-19

**Definition:** The information system provides the capability for users to directly initiate session lock mechanisms.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AC-11 a

NIST: NIST SP 800-53 Revision 4 (v4): AC-11 a

NIST: NIST SP 800-53A (v1): AC-11

---

**CCI:** CCI-000059 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-14

**Definition:** The organization defines the time period of inactivity after which the information system initiates a session lock.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-11 a

NIST: NIST SP 800-53 Revision 4 (v4): AC-11 a

NIST: NIST SP 800-53A (v1): AC-11.1 (i)

---

**CCI:** CCI-000056 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-14
**Definition:** The information system retains the session lock until the user reestablishes access using established identification and authentication procedures.
**Type:** technical
**References:** NIST: NIST SP 800-53 (v3): AC-11 b
NIST: NIST SP 800-53 Revision 4 (v4): AC-11 b
NIST: NIST SP 800-53A (v1): AC-11.1 (iii)

---

**CCI:** CCI-000060 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-05-19
**Definition:** The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.
**Type:** technical
**References:** NIST: NIST SP 800-53 (v3): AC-11 (1)
NIST: NIST SP 800-53 Revision 4 (v4): AC-11 (1)
NIST: NIST SP 800-53A (v1): AC-11 (1).1

---

**CCI:** CCI-002254 **Status:** deprecated
**Contributor:** DISA FSO **Published Date:** 2013-06-24
**Definition:** The organization defines the conditions or trigger events requiring session disconnect to be employed by the information system when automatically terminating a user session.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-12

---

**CCI:** CCI-002360 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-06-26
**Definition:** The organization defines the conditions or trigger events requiring session disconnect to be employed by the information system when automatically terminating a user session.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-12

---

**CCI:** CCI-002361 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-06-26
**Definition:** The information system automatically terminates a user session after organization-defined conditions or trigger events requiring session disconnect.
**Type:** technical
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-12

---

**CCI:** CCI-002362 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-06-26
**Definition:** The organization defines the resources requiring information system authentication in order to gain access.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-12 (1)

---

**CCI:** CCI-002363 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-06-26
**Definition:** The information system provides a logout capability for user-initiated communications sessions whenever authentication is used to gain access to organization-defined information resources.
**Type:** technical
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-12 (1)

---

**CCI:** CCI-002364 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-06-26
**Definition:** The information system displays an explicit logout message to users indicating the reliable termination of authenticated communications sessions.
**Type:** technical
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-12 (1)

---

**CCI:** CCI-000061 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-14
**Definition:** The organization identifies and defines organization-defined user actions that can be performed on the information system without identification or authentication consistent with organizational missions/business functions.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): AC-14 a
NIST: NIST SP 800-53 Revision 4 (v4): AC-14 a
NIST: NIST SP 800-53A (v1): AC-14.1 (i)

---

**CCI:** CCI-002255 **Status:** deprecated
**Contributor:** DISA FSO **Published Date:** 2013-06-24
**Definition:** The organization defines the user actions that can be performed on the information system without identification and authentication.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-14 a

---

**CCI:** CCI-000232 **Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2009-09-14

**Definition:** The organization documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification and authentication.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-14 b
NIST: NIST SP 800-53 Revision 4 (v4): AC-14 b
NIST: NIST SP 800-53A (v1): AC-14.1 (ii)

---

**CCI:** CCI-002256

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2013-06-24

**Definition:** The organization defines security attributes having organization-defined types of security attribute values which are associated with information in storage.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-16 a

---

**CCI:** CCI-002257

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2013-06-24

**Definition:** The organization defines security attributes having organization-defined types of security attribute values which are associated with information in process.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-16 a

---

**CCI:** CCI-002258

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2013-06-24

**Definition:** The organization defines security attributes, having organization-defined types of security attribute values, which are associated with information in transmission.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-16 a

---

**CCI:** CCI-002259

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2013-06-24

**Definition:** The organization defines security attribute values associated with organization-defined types of security attributes for information in storage.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-16 a

---

**CCI:** CCI-002260

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2013-06-24

**Definition:** The organization defines security attribute values associated with organization-defined types of security attributes for information in process.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-16 a

---

**CCI:** CCI-002261 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines security attribute values associated with organization-defined types of security attributes for information in transmission.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-16 a

---

**CCI:** CCI-002262 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization provides the means to associate organization-defined types of security attributes having organization-defined security attribute values with information in storage.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-16 a

---

**CCI:** CCI-002263 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization provides the means to associate organization-defined types of security attributes having organization-defined security attribute values with information in process.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-16 a

---

**CCI:** CCI-002264 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization provides the means to associate organization-defined types of security attributes having organization-defined security attribute values with information in transmission.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-16 a

---

**CCI:** CCI-002265 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization ensures that the security attribute associations are made with the information.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-16 b

---

**CCI:** CCI-002266 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-06-24
**Definition:** The organization ensures that the security attribute associations are retained with the information.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-16 b

---

**CCI:** CCI-002267 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-06-24
**Definition:** The organization defines the security attributes that are permitted for organization-defined information systems.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-16 c

---

**CCI:** CCI-002268 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-06-24
**Definition:** The organization defines the information systems for which permitted organization-defined attributes are to be established.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-16 c

---

**CCI:** CCI-002269 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-06-24
**Definition:** The organization establishes the permitted organization-defined security attributes for organization-defined information systems.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-16 c

---

**CCI:** CCI-002270 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-06-24
**Definition:** The organization defines the values or ranges permitted for each of the established security attributes.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-16 d

---

**CCI:** CCI-002271 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-06-24
**Definition:** The organization determines the permitted organization-defined values or ranges for each of the established security attributes.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-16 d

---

**CCI:** CCI-001424 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-25

**Definition:** The information system dynamically associates security attributes with organization-defined subjects in accordance with organization-defined security policies as information is created and combined.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AC-16 (1)

NIST: NIST SP 800-53 Revision 4 (v4): AC-16 (1)

NIST: NIST SP 800-53A (v1): AC-16 (1).1

---

**CCI:** CCI-002272 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The information system dynamically associates security attributes with organization-defined objects in accordance with organization-defined security policies as information is created and combined.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-16 (1)

---

**CCI:** CCI-002273 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the security policies the information system is to adhere to when dynamically associating security attributes with organization-defined subjects and objects.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-16 (1)

---

**CCI:** CCI-002274 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the subjects with which the information system is to dynamically associate security attributes as information is created and combined.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-16 (1)

---

**CCI:** CCI-002275 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the objects with which the information system is to dynamically associate security attributes as information is created and combined.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-16 (1)

---

**CCI:** CCI-001559 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2010-05-11

**Definition:** The organization identifies the individuals authorized to change the value of associated security attributes.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-16 (2)
NIST: NIST SP 800-53 Revision 4 (v4): AC-16 (2)
NIST: NIST SP 800-53A (v1): AC-16 (2).1 (i)

---

**CCI:** CCI-001425 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-25

**Definition:** The information system provides authorized individuals (or processes acting on behalf of individuals) the capability to change the value of associated security attributes.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AC-16 (2)
NIST: NIST SP 800-53 Revision 4 (v4): AC-16 (2)
NIST: NIST SP 800-53A (v1): AC-16 (2).1 (ii)

---

**CCI:** CCI-002276 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization identifies the individuals authorized to define the value of associated security attributes.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-16 (2)

---

**CCI:** CCI-002277 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The information system provides authorized individuals (or processes acting on behalf of individuals) the capability to define the value of associated security attributes.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-16 (2)

---

**CCI:** CCI-002278 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines security attributes for which the association and integrity to organization-defined subjects and objects is maintained by the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-16 (3)

---

**CCI:** CCI-002279 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines subjects for which the association and integrity of organization-defined security attributes is maintained by the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-16 (3)

---

**CCI:** CCI-002280 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines objects for which the association and integrity of organization-defined security attributes is maintained by the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-16 (3)

---

**CCI:** CCI-002281 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The information system maintains the association of organization-defined security attributes to organization-defined subjects.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-16 (3)

---

**CCI:** CCI-002282 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The information system maintains the association of organization-defined security attributes to organization-defined objects.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-16 (3)

---

**CCI:** CCI-002283 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The information system maintains the integrity of organization-defined security attributes associated with organization-defined subjects.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-16 (3)

---

**CCI:** CCI-002284 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The information system maintains the integrity of organization-defined security attributes associated with organization-defined objects.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-16 (3)

---

**CCI:** CCI-001560 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2010-05-11

**Definition:** The organization identifies individuals (or processes acting on behalf of individuals) authorized to associate organization-defined security attributes with organization-defined objects.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-16 (4)
NIST: NIST SP 800-53 Revision 4 (v4): AC-16 (4)
NIST: NIST SP 800-53A (v1): AC-16 (4).1 (i)

---

**CCI:** CCI-002285 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization identifies individuals (or processes acting on behalf of individuals) authorized to associate organization-defined security attributes with organization-defined subjects.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-16 (4)

---

**CCI:** CCI-002286 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the subjects with which organization-defined security attributes may be associated by authorized individuals (or processes acting on behalf of individuals).

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-16 (4)

---

**CCI:** CCI-002287 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the objects with which organization-defined security attributes may be associated by authorized individuals (or processes acting on behalf of individuals).

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-16 (4)

---

**CCI:** CCI-002288 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the security attributes authorized individuals (or processes acting on behalf of individuals) are permitted to associate with organization-defined subjects and objects.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-16 (4)

---

**CCI:** CCI-002289 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The information system supports the association of organization-defined security attributes with organization-defined subjects by authorized individuals (or processes acting on behalf of individuals).

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-16 (4)

---

**CCI:** CCI-002290 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The information system supports the association of organization-defined security attributes with organization-defined objects by authorized individuals (or processes acting on behalf of individuals).

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-16 (4)

---

**CCI:** CCI-001428 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-25

**Definition:** The information system displays security attributes in human-readable form on each object that the system transmits to output devices to identify organization-identified special dissemination, handling, or distribution instructions using organization-identified human-readable, standard naming conventions.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AC-16 (5)
NIST: NIST SP 800-53 Revision 4 (v4): AC-16 (5)
NIST: NIST SP 800-53A (v1): AC-16 (5).1 (iii)

---

**CCI:** CCI-001429 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-25

**Definition:** The organization identifies special dissemination, handling, or distribution instructions for identifying security attributes on output.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-16 (5)
NIST: NIST SP 800-53 Revision 4 (v4): AC-16 (5)
NIST: NIST SP 800-53A (v1): AC-16 (5).1 (i)

---

**CCI:** CCI-001430 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-25

**Definition:** The organization identifies human-readable, standard naming conventions for identifying security attributes on output.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-16 (5)

NIST: NIST SP 800-53 Revision 4 (v4): AC-16 (5)

NIST: NIST SP 800-53A (v1): AC-16 (5).1 (ii)

---

**CCI:** CCI-002291 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the security policies to be followed by personnel when associating organization-defined security attributes with organization-defined subjects and objects.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-16 (6)

---

**CCI:** CCI-002292 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the security attributes which are to be associated with organization-defined subjects and objects.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-16 (6)

---

**CCI:** CCI-002293 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the subjects to be associated, and that association maintained, with organization-defined security attributes in accordance with organization-defined security policies.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-16 (6)

---

**CCI:** CCI-002294 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the objects to be associated, and that association maintained, with organization-defined security attributes in accordance with organization-defined security policies.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-16 (6)

---

**CCI:** CCI-002295 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization allows personnel to associate organization-defined security attributes with organization-defined subjects in accordance with organization-defined security policies.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-16 (6)

---

**CCI:** CCI-002296 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization allows personnel to associate organization-defined security attributes with organization-defined objects in accordance with organization-defined security policies.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-16 (6)

---

**CCI:** CCI-002297 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization allows personnel to maintain the association of organization-defined security attributes with organization-defined subjects in accordance with organization-defined security policies.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-16 (6)

---

**CCI:** CCI-002298 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization allows personnel to maintain the association of organization-defined security attributes with organization-defined objects in accordance with organization-defined security policies.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-16 (6)

---

**CCI:** CCI-002299 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization provides a consistent interpretation of security attributes transmitted between distributed information system components.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-16 (7)

---

**CCI:** CCI-002300 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the techniques or technologies to be implemented when

| | | | |
|---|---|---|---|
| | associating security attributes with information. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-16 (8) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002301 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |
| **Definition:** | The organization defines the level of assurance to be provided when implementing organization-defined techniques or technologies in associating security attributes to information. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-16 (8) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002302 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |
| **Definition:** | The information system implements organization-defined techniques or technologies with an organization-defined level of assurance in associating security attributes to information. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-16 (8) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002303 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |
| **Definition:** | The organization defines the techniques or procedures to be employed to validate re-grading mechanisms. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-16 (9) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002304 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |
| **Definition:** | The organization ensures security attributes associated with information are reassigned only via re-grading mechanisms validated using organization-defined techniques or procedures. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-16 (9) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002305 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |
| **Definition:** | The organization identifies individuals authorized to define or change the type and value of security attributes available for association with subjects and objects. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-16 (10) | | |

---

**CCI:** CCI-002306 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The information system provides authorized individuals the capability to define or change the type of security attributes available for association with subjects.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-16 (10)

---

**CCI:** CCI-002307 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The information system provides authorized individuals the capability to define or change the value of security attributes available for association with subjects.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-16 (10)

---

**CCI:** CCI-002308 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The information system provides authorized individuals the capability to define or change the type of security attributes available for association with objects.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-16 (10)

---

**CCI:** CCI-002309 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The information system provides authorized individuals the capability to define or change the value of security attributes available for association with objects.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-16 (10)

---

**CCI:** CCI-000063 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-14

**Definition:** The organization defines allowed methods of remote access to the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-17 a

NIST: NIST SP 800-53 Revision 4 (v4): AC-17 a

NIST: NIST SP 800-53A (v1): AC-17.1 (i)

---

**CCI:** CCI-002310 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

| | | | |
|---|---|---|---|
| **Definition:** | The organization establishes and documents usage restrictions for each type of remote access allowed. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-17 a | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002311 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |
| **Definition:** | The organization establishes and documents configuration/connection requirements for each type of remote access allowed. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-17 a | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002312 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |
| **Definition:** | The organization establishes and documents implementation guidance for each type of remote access allowed. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-17 a | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000065 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-14 |
| **Definition:** | The organization authorizes remote access to the information system prior to allowing such connections. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-17 d<br>NIST: NIST SP 800-53 Revision 4 (v4): AC-17 b<br>NIST: NIST SP 800-53A (v1): AC-17.1 (iv) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000067 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-14 |
| **Definition:** | The information system monitors remote access methods. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-17 (1)<br>NIST: NIST SP 800-53 Revision 4 (v4): AC-17 (1)<br>NIST: NIST SP 800-53A (v1): AC-17 (1).1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002313 | **Status:** | deprecated |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |
| **Definition:** | The information system controls remote access methods. | | |

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-17 (1)

---

**CCI:** CCI-002314 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The information system controls remote access methods.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-17 (1)

---

**CCI:** CCI-000068 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-14

**Definition:** The information system implements cryptographic mechanisms to protect the confidentiality of remote access sessions.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AC-17 (2)
NIST: NIST SP 800-53 Revision 4 (v4): AC-17 (2)
NIST: NIST SP 800-53A (v1): AC-17 (2).1

---

**CCI:** CCI-001453 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-29

**Definition:** The information system implements cryptographic mechanisms to protect the integrity of remote access sessions.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AC-17 (2)
NIST: NIST SP 800-53 Revision 4 (v4): AC-17 (2)
NIST: NIST SP 800-53A (v1): AC-17 (2).1

---

**CCI:** CCI-001561 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2010-05-11

**Definition:** The organization defines managed access control points for remote access to the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-17 (3)
NIST: NIST SP 800-53 Revision 4 (v4): AC-17 (3)
NIST: NIST SP 800-53A (v1): AC-17 (3).1 (i)

---

**CCI:** CCI-000069 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-05-19

**Definition:** The information system routes all remote accesses through an organization-defined number of managed network access control points.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-17 (3)
NIST: NIST SP 800-53 Revision 4 (v4): AC-17 (3)
NIST: NIST SP 800-53A (v1): AC-17 (3).1 (ii)

---

**CCI:** CCI-002315 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the number of managed network access control points through which the information system routes all remote access.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-17 (3)

---

**CCI:** CCI-000070 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-05-19

**Definition:** The organization authorizes the execution of privileged commands via remote access only for organization-defined needs.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-17 (4)
NIST: NIST SP 800-53 Revision 4 (v4): AC-17 (4) (a)
NIST: NIST SP 800-53A (v1): AC-17 (4).1 (i)

---

**CCI:** CCI-002316 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization authorizes access to security-relevant information via remote access only for organization-defined needs.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-17 (4) (a)

---

**CCI:** CCI-002317 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the operational needs for when the execution of privileged commands via remote access is to be authorized.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-17 (4) (a)

---

**CCI:** CCI-002318 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the operational needs for when access to security-relevant information via remote access is to be authorized.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-17 (4) (a)

---

**CCI:** CCI-002319

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2013-06-24

**Definition:** The organization documents in the security plan for the information system the rationale for authorization of the execution of privilege commands via remote access.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-17 (4) (b)

---

**CCI:** CCI-002320

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2013-06-24

**Definition:** The organization documents in the security plan for the information system the rationale for authorization of access to security-relevant information via remote access.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-17 (4) (b)

---

**CCI:** CCI-000072

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2009-09-25

**Definition:** The organization ensures that users protect information about remote access mechanisms from unauthorized use and disclosure.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-17 (6)
NIST: NIST SP 800-53 Revision 4 (v4): AC-17 (6)
NIST: NIST SP 800-53A (v1): AC-17 (6).1

---

**CCI:** CCI-002321

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2013-06-24

**Definition:** The organization defines the time period within which it disconnects or disables remote access to the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-17 (9)

---

**CCI:** CCI-002322

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2013-06-24

**Definition:** The organization provides the capability to expeditiously disconnect or disable remote access to the information system within the organization-defined time period.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-17 (9)

---

**CCI:** CCI-001438
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2009-09-25
**Definition:** The organization establishes usage restrictions for wireless access.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): AC-18 a
NIST: NIST SP 800-53 Revision 4 (v4): AC-18 a
NIST: NIST SP 800-53A (v1): AC-18.1 (i)

---

**CCI:** CCI-001439
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2009-09-25
**Definition:** The organization establishes implementation guidance for wireless access.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): AC-18 a
NIST: NIST SP 800-53 Revision 4 (v4): AC-18 a
NIST: NIST SP 800-53A (v1): AC-18.1 (i)

---

**CCI:** CCI-002323
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2013-06-24
**Definition:** The organization establishes configuration/connection requirements for wireless access.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-18 a

---

**CCI:** CCI-001441
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2009-09-25
**Definition:** The organization authorizes wireless access to the information system prior to allowing such connections.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): AC-18 c
NIST: NIST SP 800-53 Revision 4 (v4): AC-18 b
NIST: NIST SP 800-53A (v1): AC-18.1 (iii)

---

**CCI:** CCI-001443
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2009-09-25
**Definition:** The information system protects wireless access to the system using authentication of users and/or devices.
**Type:** technical
**References:** NIST: NIST SP 800-53 (v3): AC-18 (1)

NIST: NIST SP 800-53 Revision 4 (v4): AC-18 (1)
NIST: NIST SP 800-53A (v1): AC-18 (1).1

---

**CCI:** CCI-001444 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-25
**Definition:** The information system protects wireless access to the system using encryption.
**Type:** technical
**References:** NIST: NIST SP 800-53 (v3): AC-18 (1)
NIST: NIST SP 800-53 Revision 4 (v4): AC-18 (1)
NIST: NIST SP 800-53A (v1): AC-18 (1).1

---

**CCI:** CCI-001449 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-25
**Definition:** The organization disables, when not intended for use, wireless networking capabilities internally embedded within information system components prior to issuance and deployment.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): AC-18 (3)
NIST: NIST SP 800-53 Revision 4 (v4): AC-18 (3)
NIST: NIST SP 800-53A (v1): AC-18 (3).1

---

**CCI:** CCI-002324 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-06-24
**Definition:** The organization identifies and explicitly authorizes users allowed to independently configure wireless networking capabilities.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-18 (4)

---

**CCI:** CCI-001451 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-25
**Definition:** The organization selects radio antennas and calibrates transmission power levels to reduce the probability that usable signals can be received outside of organization-controlled boundaries.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): AC-18 (5)
NIST: NIST SP 800-53 Revision 4 (v4): AC-18 (5)
NIST: NIST SP 800-53A (v1): AC-18 (5).1

---

**CCI:** CCI-000082 **Status:** draft
**Contributor:** DISA FSO **Published** 2009-05-19

| | | | |
|---|---|---|---|
| | | **Date:** | |
| **Definition:** | The organization establishes usage restrictions for organization-controlled mobile devices. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-19 a<br>NIST: NIST SP 800-53 Revision 4 (v4): AC-19 a<br>NIST: NIST SP 800-53A (v1): AC-19.1 (i) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000083 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-05-19 |
| **Definition:** | The organization establishes implementation guidance for organization-controlled mobile devices. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-19 a<br>NIST: NIST SP 800-53 Revision 4 (v4): AC-19 a<br>NIST: NIST SP 800-53A (v1): AC-19.1 (i) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002325 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |
| **Definition:** | The organization establishes configuration requirements for organization-controlled mobile devices. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-19 a | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002326 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |
| **Definition:** | The organization establishes connection requirements for organization-controlled mobile devices. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-19 a | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000084 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-14 |
| **Definition:** | The organization authorizes connection of mobile devices to organizational information systems. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-19 b<br>NIST: NIST SP 800-53 Revision 4 (v4): AC-19 b<br>NIST: NIST SP 800-53A (v1): AC-19.1 (ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001330 | **Status:** | draft |

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization prohibits the use of unclassified mobile devices in facilities containing information systems processing, storing, or transmitting classified information unless specifically permitted by the authorizing official.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-19 (4) (a)
NIST: NIST SP 800-53 Revision 4 (v4): AC-19 (4) (a)
NIST: NIST SP 800-53A (v1): AC-19 (4).1 (i)

---

**CCI:** CCI-001458 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-29

**Definition:** The organization requires that if classified information is found on mobile devices, the incident handling policy be followed.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-19 (4) (b)
NIST: NIST SP 800-53 Revision 4 (v4): AC-19 (4) (b) (4)
NIST: NIST SP 800-53A (v1): AC-19 (4).1 (iii)

---

**CCI:** CCI-001331 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization prohibits connection of unclassified mobile devices to classified information systems.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-19 (4) (b)
NIST: NIST SP 800-53 Revision 4 (v4): AC-19 (4) (b) (1)
NIST: NIST SP 800-53A (v1): AC-19 (4).1 (iii)

---

**CCI:** CCI-001332 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization requires approval from the authorizing official for the connection of unclassified mobile devices to unclassified information systems.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-19 (4) (b)
NIST: NIST SP 800-53 Revision 4 (v4): AC-19 (4) (b) (2)
NIST: NIST SP 800-53A (v1): AC-19 (4).1 (iii)

---

**CCI:** CCI-001333 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization prohibits use of internal or external modems or wireless interfaces within unclassified mobile devices in facilities containing information systems processing, storing, or transmitting classified information.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-19 (4) (b)
NIST: NIST SP 800-53 Revision 4 (v4): AC-19 (4) (b) (3)
NIST: NIST SP 800-53A (v1): AC-19 (4).1 (iii)

---

**CCI:** CCI-001334 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization requires that unclassified mobile devices used in facilities containing information systems processing, storing, or transmitting classified information and the information stored on those devices be subject to random reviews and inspections by organization-defined security officials.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-19 (4) (b)
NIST: NIST SP 800-53 Revision 4 (v4): AC-19 (4) (b) (4)
NIST: NIST SP 800-53A (v1): AC-19 (4).1 (iii)

---

**CCI:** CCI-001335 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization defines security officials to perform reviews and inspections of unclassified mobile devices in facilities containing information systems processing, storing, or transmitting classified information.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-19 (4) (b)
NIST: NIST SP 800-53 Revision 4 (v4): AC-19 (4) (b) (4)
NIST: NIST SP 800-53A (v1): AC-19 (4).1 (ii)

---

**CCI:** CCI-002327 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the security policies which restrict the connection of classified mobile devices to classified information systems.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-19 (4) (c)

---

**CCI:** CCI-002328 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization restricts the connection of classified mobile devices to classified information systems in accordance with organization-defined security policies.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-19 (4) (c)

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002329 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |
| **Definition:** | The organization defines the mobile devices that are to employ full-device or container encryption to protect the confidentiality and integrity of the information on the device. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-19 (5) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002330 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |
| **Definition:** | The organization employs full-device encryption or container encryption to protect the confidentiality of information on organization-defined mobile devices. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-19 (5) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002331 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |
| **Definition:** | The organization employs full-device encryption or container encryption to protect the integrity of information on organization-defined mobile devices. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-19 (5) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000093 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-14 |
| **Definition:** | The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to access the information system from the external information systems. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-20 a<br>NIST: NIST SP 800-53 Revision 4 (v4): AC-20 a<br>NIST: NIST SP 800-53A (v1): AC-20.1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002332 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-24 |
| **Definition:** | The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to process, store, or transmit organization-controlled information using the external information systems. | | |
| **Type:** | policy | | |

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-20 b

---

**CCI:** CCI-002333 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization permits authorized individuals to use an external information system to access the information system only when the organization verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-20 (1) (a)

---

**CCI:** CCI-002334 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization permits authorized individuals to use an external information system to process organization-controlled information only when the organization verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-20 (1) (a)

---

**CCI:** CCI-002335 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization permits authorized individuals to use an external information system to store organization-controlled information only when the organization verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-20 (1) (a)

---

**CCI:** CCI-002336 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization permits authorized individuals to use an external information system to transmit organization-controlled information only when the organization verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-20 (1) (a)

---

**CCI:** CCI-002337 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization retains approved information system connection or processing agreements with the organizational entity hosting the external information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-20 (1) (b)

---

**CCI:** CCI-000097 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-14

**Definition:** The organization restricts or prohibits the use of organization-controlled portable storage devices by authorized individuals on external information systems.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-20 (2)
NIST: NIST SP 800-53 Revision 4 (v4): AC-20 (2)
NIST: NIST SP 800-53A (v1): AC-20 (2).1

---

**CCI:** CCI-002338 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization restricts or prohibits the use of non-organizationally owned information systems, system components, or devices to process, store, or transmit organizational information.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-20 (3)

---

**CCI:** CCI-002339 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization defines the network accessible storage devices that are to be prohibited from being used in external information systems.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-20 (4)

---

**CCI:** CCI-002340 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-24

**Definition:** The organization prohibits the use of organization-defined network accessible storage devices in external information systems.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-20 (4)

---

**CCI:** CCI-000098 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-05-19

**Definition:** The organization facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for organization-defined information circumstances where user discretion is required.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-21 a
NIST: NIST SP 800-53 Revision 4 (v4): AC-21 a
NIST: NIST SP 800-53A (v1): AC-21.1 (ii)

---

**CCI:** CCI-001470 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-29

**Definition:** The organization defines information sharing circumstances where user discretion is required.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-21 a
NIST: NIST SP 800-53 Revision 4 (v4): AC-21 a
NIST: NIST SP 800-53A (v1): AC-21.1 (i)

---

**CCI:** CCI-001471 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-29

**Definition:** The organization employs organization-defined automated mechanisms or manual processes required to assist users in making information sharing/collaboration decisions.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-21 b
NIST: NIST SP 800-53 Revision 4 (v4): AC-21 b
NIST: NIST SP 800-53A (v1): AC-21.1 (iv)

---

**CCI:** CCI-001472 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-29

**Definition:** The organization defines the automated mechanisms or manual processes required to assist users in making information sharing/collaboration decisions.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-21 b
NIST: NIST SP 800-53 Revision 4 (v4): AC-21 b
NIST: NIST SP 800-53A (v1): AC-21.1 (iii)

---

**CCI:** CCI-000099 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-05-19

**Definition:** The information system enforces information-sharing decisions by authorized users based on access authorizations of sharing partners and access restrictions on information to be shared.

**Type:** policy, technical

**References:** NIST: NIST SP 800-53 (v3): AC-21 (1)
NIST: NIST SP 800-53 Revision 4 (v4): AC-21 (1)
NIST: NIST SP 800-53A (v1): AC-21 (1).1

---

**CCI:** CCI-002341 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-25

**Definition:** The organization defines the information sharing restrictions to be enforced by the information system for information search and retrieval services.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-21 (2)

---

**CCI:** CCI-002342 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-25

**Definition:** The information system implements information search and retrieval services that enforce organization-defined information sharing restrictions.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-21 (2)

---

**CCI:** CCI-001473 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-29

**Definition:** The organization designates individuals authorized to post information onto a publicly accessible information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-22 a
NIST: NIST SP 800-53 Revision 4 (v4): AC-22 a
NIST: NIST SP 800-53A (v1): AC-22.1 (i)

---

**CCI:** CCI-001474 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-29

**Definition:** The organization trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-22 b
NIST: NIST SP 800-53 Revision 4 (v4): AC-22 b
NIST: NIST SP 800-53A (v1): AC-22.1 (ii)

---

**CCI:** CCI-001475 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-29

**Definition:** The organization reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-22 c
NIST: NIST SP 800-53 Revision 4 (v4): AC-22 c
NIST: NIST SP 800-53A (v1): AC-22.1 (iii)

---

**CCI:** CCI-001476 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-29

**Definition:** The organization reviews the content on the publicly accessible information system for nonpublic information on an organization-defined frequency.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-22 d
NIST: NIST SP 800-53 Revision 4 (v4): AC-22 d
NIST: NIST SP 800-53A (v1): AC-22.1 (iv)

---

**CCI:** CCI-001477 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-29

**Definition:** The organization defines a frequency for reviewing the content on the publicly accessible information system for nonpublic information.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-22 d
NIST: NIST SP 800-53 Revision 4 (v4): AC-22 d
NIST: NIST SP 800-53A (v1): AC-22.1 (ii)

---

**CCI:** CCI-001478 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-29

**Definition:** The organization removes nonpublic information from the publicly accessible information system, if discovered.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-22 e
NIST: NIST SP 800-53 Revision 4 (v4): AC-22 d
NIST: NIST SP 800-53A (v1): AC-22.1 (v)

---

**CCI:** CCI-002343 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-25

**Definition:** The organization defines the data mining prevention techniques to be employed to adequately protect organization-defined data storage objects against data mining.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-23

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002344 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-25 |
| **Definition:** | The organization defines the data mining detection techniques to be employed to adequately detect data mining attempts against organization-defined data storage objects. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-23 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002345 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-25 |
| **Definition:** | The organization defines the data storage objects that are to be protected against data mining attempts. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-23 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002346 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-25 |
| **Definition:** | The organization employs organization-defined data mining prevention techniques for organization-defined data storage objects to adequately protect against data mining. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-23 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002347 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-25 |
| **Definition:** | The organization employs organization-defined data mining detection techniques for organization-defined data storage objects to adequately detect data mining attempts. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-23 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002348 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-25 |
| **Definition:** | The organization defines the access control decisions that are to be applied to each access request prior to access enforcement. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AC-24 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002349 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-25 |
| **Definition:** | The organization establishes procedures to ensure organization-defined access control | | |

decisions are applied to each access request prior to access enforcement.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-24

---

**CCI:** CCI-002350 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-25

**Definition:** The organization defines the access authorization information that is to be transmitted using organization-defined security safeguards to organization-defined information systems that enforce access control decisions.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-24 (1)

---

**CCI:** CCI-002351 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-25

**Definition:** The organization defines the security safeguards to be employed when transmitting organization-defined access authorization information to organization-defined information systems that enforce access control decisions.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-24 (1)

---

**CCI:** CCI-002352 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-25

**Definition:** The organization defines the information systems that are to be recipients of organization-defined access authorization information using organization-defined security safeguards.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-24 (1)

---

**CCI:** CCI-002353 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-25

**Definition:** The information system transmits organization-defined access authorization information using organization-defined security safeguards to organization-defined information systems which enforce access control decisions.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-24 (1)

---

**CCI:** CCI-002354 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-25

**Definition:** The organization defines the security attributes, not to include the identity of the user or process acting on behalf of the user, to be used as the basis for enforcing access control decisions.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-24 (2)

---

**CCI:** CCI-002355 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-25

**Definition:** The information system enforces access control decisions based on organization-defined security attributes that do not include the identity of the user or process acting on behalf of the user.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-24 (2)

---

**CCI:** CCI-002356 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-25

**Definition:** The organization defines the access control policies to be implemented by the information system's reference monitor.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-25

---

**CCI:** CCI-002357 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-25

**Definition:** The information system implements a reference monitor for organization-defined access control policies that is tamperproof.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-25

---

**CCI:** CCI-002358 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-25

**Definition:** The information system implements a reference monitor for organization-defined access control policies that is always invoked.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-25

---

**CCI:** CCI-002359 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-25

**Definition:** The information system implements a reference monitor for organization-defined access control policies that is small enough to be subject to analysis and testing, the completeness of which can be assured.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AC-25

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003392 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-07 |
| **Definition:** | The organization determines and documents the legal authority that permits the collection of personally identifiable information (PII), either generally or in support of a specific program or information system need. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AP-1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003393 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-07 |
| **Definition:** | The organization determines and documents the legal authority that permits the use of personally identifiable information (PII), either generally or in support of a specific program or information system need. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AP-1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003394 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-07 |
| **Definition:** | The organization determines and documents the legal authority that permits the maintenance of personally identifiable information (PII), either generally or in support of a specific program or information system need. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AP-1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003395 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-07 |
| **Definition:** | The organization determines and documents the legal authority that permits the sharing of personally identifiable information (PII), either generally or in support of a specific program or information system need. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AP-1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003396 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-07 |
| **Definition:** | The organization describes, in its privacy notices, the purpose(s) for which personally identifiable information (PII) is collected. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AP-2 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003398 | **Status:** | draft |

**Contributor:** DISA FSO
**Published Date:** 2013-11-07
**Definition:** The organization describes, in its privacy notices, the purpose(s) for which personally identifiable information (PII) is used.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AP-2

---

**CCI:** CCI-003399
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2013-11-07
**Definition:** The organization describes, in its privacy notices, the purpose(s) for which personally identifiable information (PII) is maintained.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AP-2

---

**CCI:** CCI-003400
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2013-11-07
**Definition:** The organization describes, in its privacy notices, the purpose(s) for which personally identifiable information (PII) is shared.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AP-2

---

**CCI:** CCI-003397
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2013-11-07
**Definition:** The organization appoints a Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) accountable for developing, implementing, and maintaining an organization-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of personally identifiable information (PII) by programs and information systems.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AR-1 a

---

**CCI:** CCI-003401
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2013-11-07
**Definition:** The organization monitors federal privacy laws and policy for changes that affect the privacy program.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AR-1 b

---

**CCI:** CCI-003402
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2013-11-07

**Definition:** The organization defines the allocation of budget resources sufficient to implement and operate the organization-wide privacy program.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AR-1 c

---

**CCI:** CCI-003403 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

**Definition:** The organization defines the allocation of staffing resources sufficient to implement and operate the organization-wide privacy program.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AR-1 c

---

**CCI:** CCI-003404 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

**Definition:** The organization allocates sufficient organization-defined budget resources to implement and operate the organization-wide privacy program.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AR-1 c

---

**CCI:** CCI-003405 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

**Definition:** The organization allocates sufficient organization-defined staffing resources to implement and operate the organization-wide privacy program.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AR-1 c

---

**CCI:** CCI-003406 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

**Definition:** The organization develops a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AR-1 d

---

**CCI:** CCI-003407 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

**Definition:** The organization develops operational privacy policies which govern the appropriate privacy and security controls for programs, information systems, or technologies involving personally identifiable information (PII).

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AR-1 e

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003408 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-07 |
| **Definition:** | The organization disseminates operational privacy policies which govern the appropriate privacy and security controls for programs, information systems, or technologies involving personally identifiable information (PII). | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AR-1 e | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003409 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-07 |
| **Definition:** | The organization implements operational privacy policies which govern the appropriate privacy and security controls for programs, information systems, or technologies involving personally identifiable information (PII). | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AR-1 e | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003410 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-07 |
| **Definition:** | The organization develops operational privacy procedures which govern the appropriate privacy and security controls for programs, information systems, or technologies involving personally identifiable information (PII). | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AR-1 e | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003411 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-07 |
| **Definition:** | The organization disseminates operational privacy procedures which govern the appropriate privacy and security controls for programs, information systems, or technologies involving personally identifiable information (PII). | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AR-1 e | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003412 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-07 |
| **Definition:** | The organization implements operational privacy procedures which govern the appropriate privacy and security controls for programs, information systems, or technologies involving personally identifiable information (PII). | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AR-1 e | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003413 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-07 |
| **Definition:** | The organization defines the frequency, minimally biennially, on which the privacy plan, policies, and procedures are to be updated. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AR-1 f | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003414 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-07 |
| **Definition:** | The organization updates the privacy plan per organization-defined frequency. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AR-1 f | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003415 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-07 |
| **Definition:** | The organization updates the privacy policies per organization-defined frequency. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AR-1 f | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003416 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-07 |
| **Definition:** | The organization updates the privacy procedures per organization-defined frequency. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AR-1 f | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003417 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-07 |
| **Definition:** | The organization documents a privacy risk management process which assesses the privacy risk to individuals. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AR-2 a | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003418 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-07 |
| **Definition:** | The organization implements a privacy risk management process which assesses the privacy risk to individuals. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AR-2 a | | |

**CCI:** CCI-003419 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

**Definition:** The organization's privacy risk management process assesses the privacy risk to individuals resulting from the collection of personally identifiable information (PII).

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AR-2 a

---

**CCI:** CCI-003420 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

**Definition:** The organization's privacy risk management process assesses the privacy risk to individuals resulting from the sharing of personally identifiable information (PII).

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AR-2 a

---

**CCI:** CCI-003421 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

**Definition:** The organization's privacy risk management process assesses the privacy risk to individuals resulting from the storing of personally identifiable information (PII).

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AR-2 a

---

**CCI:** CCI-003422 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

**Definition:** The organization's privacy risk management process assesses the privacy risk to individuals resulting from the transmitting of personally identifiable information (PII).

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AR-2 a

---

**CCI:** CCI-003423 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

**Definition:** The organization's privacy risk management process assesses the privacy risk to individuals resulting from the use of personally identifiable information (PII).

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AR-2 a

---

**CCI:** CCI-003424 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

**Definition:** The organization's privacy risk management process assesses the privacy risk to individuals resulting from the disposal of personally identifiable information (PII).

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AR-2 a

---

**CCI:** CCI-003425 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

**Definition:** The organization conducts Privacy Impact Assessments (PIAs) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AR-2 b

---

**CCI:** CCI-003426 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

**Definition:** The organization establishes privacy roles for contractors.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AR-3 a

---

**CCI:** CCI-003427 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

**Definition:** The organization establishes privacy responsibilities for contractors.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AR-3 a

---

**CCI:** CCI-003428 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

**Definition:** The organization establishes access requirements for contractors.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AR-3 a

---

**CCI:** CCI-003429 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

**Definition:** The organization establishes privacy roles for service providers.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AR-3 a

---

**CCI:** CCI-003430 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

| | | | |
|---|---|---|---|
| **Definition:** | The organization establishes privacy responsibilities for service providers. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AR-3 a | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003431 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-07 |
| **Definition:** | The organization establishes access requirements for service providers. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AR-3 a | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003432 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-07 |
| **Definition:** | The organization includes privacy requirements in contracts. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AR-3 b | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003433 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-07 |
| **Definition:** | The organization includes privacy requirements in other acquisition-related documents. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AR-3 b | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003434 | **Status:** | deprecated |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-07 |
| **Definition:** | The organization defines the frequency for monitoring privacy controls and internal privacy policy to ensure effective implementation. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AR-4 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003435 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-07 |
| **Definition:** | The organization defines the frequency for auditing privacy controls and internal privacy policy to ensure effective implementation. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AR-4 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003436 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-07 |

**Definition:** The organization monitors privacy controls, per organization-defined frequency, to ensure effective implementation.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AR-4

**CCI:** CCI-003437 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

**Definition:** The organization monitors internal privacy policy to ensure effective implementation.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AR-4

**CCI:** CCI-003438 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

**Definition:** The organization audits privacy controls, per organization-defined frequency, to ensure effective implementation.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AR-4

**CCI:** CCI-003439 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

**Definition:** The organization audits internal privacy policy, per organization-defined frequency, to ensure effective implementation.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AR-4

**CCI:** CCI-003440 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

**Definition:** The organization develops a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AR-5 a

**CCI:** CCI-003441 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

**Definition:** The organization implements a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AR-5 a

**CCI:** CCI-003442 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

**Definition:** The organization updates a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AR-5 a

---

**CCI:** CCI-003443 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

**Definition:** The organization defines the frequency, minimally annually, for administering its basic privacy training.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AR-5 b

---

**CCI:** CCI-003444 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

**Definition:** The organization defines the frequency, minimally annually, for administering the targeted, role-based privacy training for personnel having responsibility for personally identifiable information (PII) or for activities that involve PII.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AR-5 b

---

**CCI:** CCI-003445 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

**Definition:** The organization administers basic privacy training per the organization-defined frequency.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AR-5 b

---

**CCI:** CCI-003446 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

**Definition:** The organization administers, per organization-defined frequency, targeted, role-based privacy training for personnel having responsibility for personally identifiable information (PII) or for activities that involve PII.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AR-5 b

---

**CCI:** CCI-003447 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

**Definition:** The organization defines the frequency, minimally annually, on which personnel certify acceptance of responsibilities for privacy requirements.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AR-5 c

---

**CCI:** CCI-003448 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

**Definition:** The organization ensures personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements per organization-defined frequency.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AR-5 c

---

**CCI:** CCI-003449 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

**Definition:** The organization develops reports for the Office of Management and Budget (OMB), Congress, and other oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory privacy program mandates.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AR-6

---

**CCI:** CCI-003450 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

**Definition:** The organization disseminates reports to the Office of Management and Budget (OMB), Congress, and other oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory privacy program mandates.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AR-6

---

**CCI:** CCI-003451 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

**Definition:** The organization updates reports for the Office of Management and Budget (OMB), Congress, and other oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory privacy program mandates.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AR-6

---

**CCI:** CCI-003452 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

**Definition:** The organization develops reports for senior management and other personnel with responsibility for monitoring privacy program progress and compliance.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AR-6

**CCI:** CCI-003453 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-11-07
**Definition:** The organization disseminates reports to senior management and other personnel with responsibility for monitoring privacy program progress and compliance.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AR-6

---

**CCI:** CCI-003454 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-11-07
**Definition:** The organization updates reports for senior management and other personnel with responsibility for monitoring privacy program progress and compliance.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AR-6

---

**CCI:** CCI-003455 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-11-07
**Definition:** The organization designs information systems to support privacy by automating privacy controls.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AR-7

---

**CCI:** CCI-003456 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-11-07
**Definition:** The organization, as part of the accurate accounting of disclosures of Privacy Act information held in each system of records under its control, includes the date of each disclosure of a record.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AR-8 a (1)

---

**CCI:** CCI-003457 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-11-07
**Definition:** The organization, as part of the accurate accounting of disclosures of Privacy Act information held in each system of records under its control, includes the nature of each disclosure of a record.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AR-8 a (1)

---

**CCI:** CCI-003458 **Status:** draft
**Contributor:** DISA FSO **Published** 2013-11-07

**Date:**

**Definition:** The organization, as part of the accurate accounting of disclosures of Privacy Act information held in each system of records under its control, includes the purpose of each disclosure of a record.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AR-8 a (1)

---

**CCI:** CCI-003459 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

**Definition:** The organization keeps an accurate accounting of disclosures of Privacy Act information held in each system of records under its control.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AR-8 a (1)

---

**CCI:** CCI-003460 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

**Definition:** The organization, as part of the accurate accounting of disclosures of Privacy Act information held in each system of records under its control, includes the name and address of the person or agency to which the disclosure was made.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AR-8 a (2)

---

**CCI:** CCI-003461 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

**Definition:** The organization retains the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AR-8 b

---

**CCI:** CCI-003462 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

**Definition:** The organization makes the accounting of disclosures available to the person named in the record upon request.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AR-8 c

---

**CCI:** CCI-000100 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-05-20

**Definition:** The organization develops and documents a security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination

| | | | |
|---|---|---|---|
| | among organizational entities, and compliance. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AT-1 a<br>NIST: NIST SP 800-53 Revision 4 (v4): AT-1 a 1<br>NIST: NIST SP 800-53A (v1): AT-1.1 (i and ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000101 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-05-20 |
| **Definition:** | The organization disseminates a security awareness and training policy to organization-defined personnel or roles. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AT-1 a<br>NIST: NIST SP 800-53 Revision 4 (v4): AT-1 a 1<br>NIST: NIST SP 800-53A (v1): AT-1.1 (iii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000103 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-05-20 |
| **Definition:** | The organization develops and documents procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AT-1 b<br>NIST: NIST SP 800-53 Revision 4 (v4): AT-1 a 2<br>NIST: NIST SP 800-53A (v1): AT-1.1 (iv and v) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000104 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-05-20 |
| **Definition:** | The organization disseminates security awareness and training procedures to organization-defined personnel or roles. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AT-1 b<br>NIST: NIST SP 800-53 Revision 4 (v4): AT-1 a 2<br>NIST: NIST SP 800-53A (v1): AT-1.1 (vi) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002048 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-05 |
| **Definition:** | The organization defines the personnel or roles to whom the security awareness and training policy is disseminated. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AT-1 a 1 | | |

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-002049 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-05 |

**Definition:** The organization defines the personnel or roles to whom the security awareness and training procedures are disseminated.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AT-1 a 2

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-001564 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-11 |

**Definition:** The organization defines the frequency of security awareness and training policy reviews and updates.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AT-1 a
NIST: NIST SP 800-53 Revision 4 (v4): AT-1 b 1
NIST: NIST SP 800-53A (v1): AT-1.2 (i)

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-001565 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-11 |

**Definition:** The organization defines the frequency of security awareness and training procedure reviews and updates.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AT-1 b
NIST: NIST SP 800-53 Revision 4 (v4): AT-1 b 2
NIST: NIST SP 800-53A (v1): AT-1.2 (iii)

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-000102 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-05-20 |

**Definition:** The organization reviews and updates the current security awareness and training policy in accordance with organization-defined frequency.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AT-1 a
NIST: NIST SP 800-53 Revision 4 (v4): AT-1 b 1
NIST: NIST SP 800-53A (v1): AT-1.2 (ii)

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-000105 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-05-20 |

**Definition:** The organization reviews and updates the current security awareness and training procedures in accordance with an organization-defined frequency.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AT-1 b
NIST: NIST SP 800-53 Revision 4 (v4): AT-1 b 2
NIST: NIST SP 800-53A (v1): AT-1.2 (iii)

---

**CCI:** CCI-001480 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-29
**Definition:** The organization defines the frequency for providing refresher security awareness training to all information system users (including managers, senior executives, and contractors).
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): AT-2
NIST: NIST SP 800-53 Revision 4 (v4): AT-2
NIST: NIST SP 800-53A (v1): AT-2.1 (ii)

---

**CCI:** CCI-000106 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-14
**Definition:** The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors) as part of initial training for new users.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): AT-2
NIST: NIST SP 800-53 Revision 4 (v4): AT-2 a
NIST: NIST SP 800-53A (v1): AT-2.1 (i)

---

**CCI:** CCI-000112 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-05-20
**Definition:** The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors) when required by information system changes.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): AT-2
NIST: NIST SP 800-53 Revision 4 (v4): AT-2 b
NIST: NIST SP 800-53A (v1): AT-2.1 (i)

---

**CCI:** CCI-001479 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-29
**Definition:** The organization provides refresher security awareness training to all information system users (including managers, senior executives, and contractors) in accordance with the organization-defined frequency.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): AT-2

NIST: NIST SP 800-53 Revision 4 (v4): AT-2 c
NIST: NIST SP 800-53A (v1): AT-2.1 (iii)

---

**CCI:** CCI-000107
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2009-05-20
**Definition:** The organization includes practical exercises in security awareness training that simulate actual cyber attacks.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): AT-2 (1)
NIST: NIST SP 800-53 Revision 4 (v4): AT-2 (1)
NIST: NIST SP 800-53A (v1): AT-2 (1).1

---

**CCI:** CCI-002055
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2013-06-05
**Definition:** The organization includes security awareness training on recognizing and reporting potential indicators of insider threat.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AT-2 (2)

---

**CCI:** CCI-000108
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2009-05-20
**Definition:** The organization provides role-based security training to personnel with assigned security roles and responsibilities before authorizing access to the information system or performing assigned duties.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): AT-3
NIST: NIST SP 800-53 Revision 4 (v4): AT-3 a
NIST: NIST SP 800-53A (v1): AT-3.1 (i)

---

**CCI:** CCI-000109
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2009-05-20
**Definition:** The organization provides role-based security training to personnel with assigned security roles and responsibilities when required by information system changes.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): AT-3
NIST: NIST SP 800-53 Revision 4 (v4): AT-3 b
NIST: NIST SP 800-53A (v1): AT-3.1 (i)

---

**CCI:** CCI-000110
**Status:** draft
**Contributor:** DISA FSO
**Published** 2009-05-20

| | | | |
|---|---|---|---|
| | | **Date:** | |
| **Definition:** | The organization provides refresher role-based security training to personnel with assigned security roles and responsibilities in accordance with organization-defined frequency. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AT-3<br>NIST: NIST SP 800-53 Revision 4 (v4): AT-3 c<br>NIST: NIST SP 800-53A (v1): AT-3.1 (iii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000111 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-05-20 |
| **Definition:** | The organization defines a frequency for providing refresher role-based security training. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AT-3<br>NIST: NIST SP 800-53 Revision 4 (v4): AT-3 c<br>NIST: NIST SP 800-53A (v1): AT-3.1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001481 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-29 |
| **Definition:** | The organization provides organization-defined personnel or roles with initial training in the employment and operation of environmental controls. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AT-3 (1)<br>NIST: NIST SP 800-53 Revision 4 (v4): AT-3 (1)<br>NIST: NIST SP 800-53A (v1): AT-3 (1).1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001482 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-29 |
| **Definition:** | The organization provides organization-defined personnel or roles with refresher training in the employment and operation of environmental controls in accordance with the organization-defined frequency. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AT-3 (1)<br>NIST: NIST SP 800-53 Revision 4 (v4): AT-3 (1)<br>NIST: NIST SP 800-53A (v1): AT-3 (1).1 (iii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001483 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-29 |
| **Definition:** | The organization defines a frequency for providing employees with refresher training in the employment and operation of environmental controls. | | |
| **Type:** | policy | | |

**References:** NIST: NIST SP 800-53 (v3): AT-3 (1)
NIST: NIST SP 800-53 Revision 4 (v4): AT-3 (1)
NIST: NIST SP 800-53A (v1): AT-3 (1).1 (ii)

---

**CCI:** CCI-002050 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-06-05
**Definition:** The organization defines the personnel or roles to whom initial and refresher training in the employment and operation of environmental controls is to be provided.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AT-3 (1)

---

**CCI:** CCI-001566 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2010-05-11
**Definition:** The organization provides organization-defined personnel or roles with initial training in the employment and operation of physical security controls.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): AT-3 (2)
NIST: NIST SP 800-53 Revision 4 (v4): AT-3 (2)
NIST: NIST SP 800-53A (v1): AT-3 (2).1 (i)

---

**CCI:** CCI-001567 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2010-05-11
**Definition:** The organization provides organization-defined personnel or roles with refresher training in the employment and operation of physical security controls in accordance with the organization-defined frequency.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): AT-3 (2)
NIST: NIST SP 800-53 Revision 4 (v4): AT-3 (2)
NIST: NIST SP 800-53A (v1): AT-3 (2).1 (iii)

---

**CCI:** CCI-001568 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2010-05-11
**Definition:** The organization defines a frequency for providing employees with refresher training in the employment and operation of physical security controls.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): AT-3 (2)
NIST: NIST SP 800-53 Revision 4 (v4): AT-3 (2)
NIST: NIST SP 800-53A (v1): AT-3 (2).1 (ii)

---

**CCI:** CCI-002051 **Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2013-06-05

**Definition:** The organization defines the personnel or roles to whom initial and refresher training in the employment and operation of physical security controls is to be provided.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AT-3 (2)

---

**CCI:** CCI-002052

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2013-06-05

**Definition:** The organization includes practical exercises in security training that reinforce training objectives.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AT-3 (3)

---

**CCI:** CCI-002053

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2013-06-05

**Definition:** The organization provides training to its personnel on organization-defined indicators of malicious code to recognize suspicious communications and anomalous behavior in organizational information systems.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AT-3 (4)

---

**CCI:** CCI-002054

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2013-06-05

**Definition:** The organization defines indicators of malicious code to recognize suspicious communications and anomalous behavior in organizational information systems.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AT-3 (4)

---

**CCI:** CCI-000113

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2009-09-14

**Definition:** The organization documents individual information system security training activities, including basic security awareness training and specific information system security training.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AT-4 a
NIST: NIST SP 800-53 Revision 4 (v4): AT-4 a
NIST: NIST SP 800-53A (v1): AT-4.1 (i)

---

**CCI:** CCI-000114

**Status:** draft

**Contributor:** DISA FSO

**Published** 2009-09-14

| | | | |
|---|---|---|---|
| | | **Date:** | |
| **Definition:** | The organization monitors individual information system security training activities, including basic security awareness training and specific information system security training. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AT-4 a<br>NIST: NIST SP 800-53 Revision 4 (v4): AT-4 a<br>NIST: NIST SP 800-53A (v1): AT-4.1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001336 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization retains individual training records for an organization-defined time period. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AT-4 b<br>NIST: NIST SP 800-53 Revision 4 (v4): AT-4 b<br>NIST: NIST SP 800-53A (v1): AT-4.1 (iii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001337 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization defines a time period for retaining individual training records. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AT-4 b<br>NIST: NIST SP 800-53 Revision 4 (v4): AT-4 b<br>NIST: NIST SP 800-53A (v1): AT-4.1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000117 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-05-20 |
| **Definition:** | The organization develops and documents an audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AU-1 a<br>NIST: NIST SP 800-53 Revision 4 (v4): AU-1 a 1<br>NIST: NIST SP 800-53A (v1): AU-1.1 (I and ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000120 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-05-20 |
| **Definition:** | The organization develops and documents procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AU-1 b | | |

NIST: NIST SP 800-53 Revision 4 (v4): AU-1 a 2
NIST: NIST SP 800-53A (v1): AU-1.1 (iv and v)

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001831 | **Status:** | deprecated |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-03-14 |
| **Definition:** | The organization documents an audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AU-1 a 1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001832 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-03-14 |
| **Definition:** | The organization disseminates the audit and accountability policy to organization-defined personnel or roles. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AU-1 a 1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001833 | **Status:** | deprecated |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-03-14 |
| **Definition:** | The organization documents procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AU-1 a 2 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001834 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-03-14 |
| **Definition:** | The organization disseminates to organization-defined personnel or roles procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AU-1 a 2 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001930 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-04-08 |
| **Definition:** | The organization defines the organizational personnel or roles to whom the audit and accountability policy is to be disseminated. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AU-1 a 1 | | |

**CCI:** CCI-001931 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-04-08

**Definition:** The organization defines the organizational personnel or roles to whom the audit and accountability procedures are to be disseminated.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-1 a 2

---

**CCI:** CCI-001569 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2010-05-11

**Definition:** The organization defines the frequency on which it will review and update the audit and accountability policy.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AU-1 a
NIST: NIST SP 800-53 Revision 4 (v4): AU-1 b 1
NIST: NIST SP 800-53A (v1): AU-1.2 (i)

---

**CCI:** CCI-001570 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2010-05-11

**Definition:** The organization defines the frequency on which it will review and update the audit and accountability procedures.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AU-1 b
NIST: NIST SP 800-53 Revision 4 (v4): AU-1 b 2
NIST: NIST SP 800-53A (v1): AU-1.2 (iii)

---

**CCI:** CCI-000119 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-05-20

**Definition:** The organization reviews and updates the audit and accountability policy on an organization-defined frequency.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AU-1 a
NIST: NIST SP 800-53 Revision 4 (v4): AU-1 b 1
NIST: NIST SP 800-53A (v1): AU-1.2 (ii)

---

**CCI:** CCI-000122 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-05-20

**Definition:** The organization reviews and updates the audit and accountability procedures on an organization-defined frequency.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AU-1 b
NIST: NIST SP 800-53 Revision 4 (v4): AU-1 b 2
NIST: NIST SP 800-53A (v1): AU-1.2 (iv)

---

**CCI:** CCI-001835 **Status:** deprecated
**Contributor:** DISA FSO **Published Date:** 2013-03-14
**Definition:** The organization defines the frequency on which it will review the audit and accountability policy.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-1 b 1

---

**CCI:** CCI-001836 **Status:** deprecated
**Contributor:** DISA FSO **Published Date:** 2013-03-14
**Definition:** The organization defines the frequency on which it will update the audit and accountability policy.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-1 b 1

---

**CCI:** CCI-001837 **Status:** deprecated
**Contributor:** DISA FSO **Published Date:** 2013-03-14
**Definition:** The organization reviews the audit and accountability policy on an organization-defined frequency.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-1 b 1

---

**CCI:** CCI-001838 **Status:** deprecated
**Contributor:** DISA FSO **Published Date:** 2013-03-14
**Definition:** The organization updates the audit and accountability policy on an organization-defined frequency.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-1 b 1

---

**CCI:** CCI-001839 **Status:** deprecated
**Contributor:** DISA FSO **Published Date:** 2013-03-14
**Definition:** The organization defines the frequency on which it will review the audit and accountability procedures.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-1 b 2

---

**CCI:** CCI-001840 **Status:** deprecated

**Contributor:** DISA FSO **Published Date:** 2013-03-14

**Definition:** The organization defines the frequency on which it will update the audit and accountability procedures.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-1 b 2

---

**CCI:** CCI-001841 **Status:** deprecated

**Contributor:** DISA FSO **Published Date:** 2013-03-14

**Definition:** The organization reviews the audit and accountability procedures on an organization-defined frequency.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-1 b 2

---

**CCI:** CCI-001842 **Status:** deprecated

**Contributor:** DISA FSO **Published Date:** 2013-03-14

**Definition:** The organization updates the audit and accountability procedures on an organization-defined frequency.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-1 b 2

---

**CCI:** CCI-001571 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2010-05-11

**Definition:** The organization defines the information system auditable events.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AU-2 a
NIST: NIST SP 800-53 Revision 4 (v4): AU-2 a
NIST: NIST SP 800-53A (v1): AU-2.1 (i)

---

**CCI:** CCI-000123 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-15

**Definition:** The organization determines the information system must be capable of auditing an organization-defined list of auditable events.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AU-2 a
NIST: NIST SP 800-53 Revision 4 (v4): AU-2 a
NIST: NIST SP 800-53A (v1): AU-2.1 (ii)

---

**CCI:** CCI-000124 **Status:** draft

**Contributor:** DISA FSO **Published** 2009-09-15

| | | | |
|---|---|---|---|
| | | **Date:** | |
| **Definition:** | The organization coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AU-2 b<br>NIST: NIST SP 800-53 Revision 4 (v4): AU-2 b<br>NIST: NIST SP 800-53A (v1): AU-2.1 (iii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000125 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-15 |
| **Definition:** | The organization provides a rationale for why the list of auditable events is deemed to be adequate to support after-the-fact investigations of security incidents. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AU-2 c<br>NIST: NIST SP 800-53 Revision 4 (v4): AU-2 c<br>NIST: NIST SP 800-53A (v1): AU-2.1 (iv) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000126 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-15 |
| **Definition:** | The organization determines that the organization-defined subset of the auditable events defined in AU-2 are to be audited within the information system. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AU-2 d<br>NIST: NIST SP 800-53 Revision 4 (v4): AU-2 d<br>NIST: NIST SP 800-53A (v1): AU-2.1 (v) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001484 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-29 |
| **Definition:** | The organization defines frequency of (or situation requiring) auditing for each identified event. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AU-2 d<br>NIST: NIST SP 800-53 Revision 4 (v4): AU-2 d<br>NIST: NIST SP 800-53A (v1): AU-2.1 (v) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001485 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-29 |
| **Definition:** | The organization defines the events which are to be audited on the information system on an organization-defined frequency of (or situation requiring) auditing for each identified | | |

event.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AU-2 d
NIST: NIST SP 800-53 Revision 4 (v4): AU-2 d
NIST: NIST SP 800-53A (v1): AU-2.1 (vi)

---

**CCI:** CCI-000127 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-05-20

**Definition:** The organization reviews and updates the list of organization-defined audited events on an organization-defined frequency.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AU-2 (3)
NIST: NIST SP 800-53 Revision 4 (v4): AU-2 (3)
NIST: NIST SP 800-53A (v1): AU-2 (3).1 (ii)

---

**CCI:** CCI-001486 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-29

**Definition:** The organization defines a frequency for reviewing and updating the list of organization-defined auditable events.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AU-2 (3)
NIST: NIST SP 800-53 Revision 4 (v4): AU-2 (3)
NIST: NIST SP 800-53A (v1): AU-2 (3).1 (i)

---

**CCI:** CCI-001843 **Status:** deprecated

**Contributor:** DISA FSO **Published Date:** 2013-03-14

**Definition:** The organization defines a frequency for updating the list of organization-defined auditable events.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-2 (3)

---

**CCI:** CCI-000130 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-05-20

**Definition:** The information system generates audit records containing information that establishes what type of event occurred.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AU-3
NIST: NIST SP 800-53 Revision 4 (v4): AU-3
NIST: NIST SP 800-53A (v1): AU-3.1

---

**CCI:** CCI-000131
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2009-05-20
**Definition:** The information system generates audit records containing information that establishes when an event occurred.
**Type:** technical
**References:** NIST: NIST SP 800-53 (v3): AU-3
NIST: NIST SP 800-53 Revision 4 (v4): AU-3
NIST: NIST SP 800-53A (v1): AU-3.1

---

**CCI:** CCI-000132
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2009-05-20
**Definition:** The information system generates audit records containing information that establishes where the event occurred.
**Type:** technical
**References:** NIST: NIST SP 800-53 (v3): AU-3
NIST: NIST SP 800-53 Revision 4 (v4): AU-3
NIST: NIST SP 800-53A (v1): AU-3.1

---

**CCI:** CCI-000133
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2009-05-20
**Definition:** The information system generates audit records containing information that establishes the source of the event.
**Type:** technical
**References:** NIST: NIST SP 800-53 (v3): AU-3
NIST: NIST SP 800-53 Revision 4 (v4): AU-3
NIST: NIST SP 800-53A (v1): AU-3.1

---

**CCI:** CCI-000134
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2009-05-20
**Definition:** The information system generates audit records containing information that establishes the outcome of the event.
**Type:** technical
**References:** NIST: NIST SP 800-53 (v3): AU-3
NIST: NIST SP 800-53 Revision 4 (v4): AU-3
NIST: NIST SP 800-53A (v1): AU-3.1

---

**CCI:** CCI-001487
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2009-09-29
**Definition:** The information system generates audit records containing information that establishes the

identity of any individuals or subjects associated with the event.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AU-3
NIST: NIST SP 800-53 Revision 4 (v4): AU-3
NIST: NIST SP 800-53A (v1): AU-3.1

---

**CCI:** CCI-000135 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-05-20

**Definition:** The information system generates audit records containing the organization-defined additional, more detailed information that is to be included in the audit records.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AU-3 (1)
NIST: NIST SP 800-53 Revision 4 (v4): AU-3 (1)
NIST: NIST SP 800-53A (v1): AU-3 (1).1 (ii)

---

**CCI:** CCI-001488 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-29

**Definition:** The organization defines additional, more detailed information to be included in the audit records.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AU-3 (1)
NIST: NIST SP 800-53 Revision 4 (v4): AU-3 (1)
NIST: NIST SP 800-53A (v1): AU-3 (1).1 (i)

---

**CCI:** CCI-001844 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-03-14

**Definition:** The information system provides centralized management and configuration of the content to be captured in audit records generated by organization-defined information system components.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-3 (2)

---

**CCI:** CCI-001845 **Status:** deprecated

**Contributor:** DISA FSO **Published Date:** 2013-03-14

**Definition:** The information system provides centralized configuration of the content to be captured in audit records generated by organization-defined information system components.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-3 (2)

---

**CCI:** CCI-001846 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-03-14

**Definition:** The organization defines information system components that will generate the audit records which are to be captured for centralized management of the content.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-3 (2)

---

**CCI:** CCI-001847 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-03-14

**Definition:** The organization defines information system components that will generate the audit records which are to be captured for centralized configuration of the content.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-3 (2)

---

**CCI:** CCI-001848 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-03-14

**Definition:** The organization defines the audit record storage requirements.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-4

---

**CCI:** CCI-001849 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-03-14

**Definition:** The organization allocates audit record storage capacity in accordance with organization-defined audit record storage requirements.

**Type:** policy, technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-4

---

**CCI:** CCI-001850 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-03-14

**Definition:** The organization defines the frequency on which the information system off-loads audit records onto a different system or media than the system being audited.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-4 (1)

---

**CCI:** CCI-001851 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-03-14

**Definition:** The information system off-loads audit records per organization-defined frequency onto a different system or media than the system being audited.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-4 (1)

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001572 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-11 |
| **Definition:** | The organization defines the personnel or roles to be alerted in the event of an audit processing failure. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AU-5 a<br>NIST: NIST SP 800-53 Revision 4 (v4): AU-5 a<br>NIST: NIST SP 800-53A (v1): AU-5.1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000139 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-15 |
| **Definition:** | The information system alerts designated organization-defined personnel or roles in the event of an audit processing failure. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): AU-5 a<br>NIST: NIST SP 800-53 Revision 4 (v4): AU-5 a<br>NIST: NIST SP 800-53A (v1): AU-5.1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000140 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-05-20 |
| **Definition:** | The information system takes organization-defined actions upon audit failure (e.g., shut down information system, overwrite oldest audit records, stop generating audit records). | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): AU-5 b<br>NIST: NIST SP 800-53 Revision 4 (v4): AU-5 b<br>NIST: NIST SP 800-53A (v1): AU-5.1 (iv) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001490 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-29 |
| **Definition:** | The organization defines actions to be taken by the information system upon audit failure (e.g., shut down information system, overwrite oldest audit records, stop generating audit records). | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AU-5 b<br>NIST: NIST SP 800-53 Revision 4 (v4): AU-5 b<br>NIST: NIST SP 800-53A (v1): AU-5.1 (iii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001852 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published** | 2013-03-14 |

**Date:**

**Definition:** The organization defines the personnel, roles and/or locations to receive a warning when allocated audit record storage volume reaches a defined percentage of maximum audit records storage capacity.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-5 (1)

---

**CCI:** CCI-001853 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-03-14

**Definition:** The organization defines the time period within which organization-defined personnel, roles, and/or locations are to receive warnings when allocated audit record storage volume reaches an organization-defined percentage of maximum audit records storage capacity.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-5 (1)

---

**CCI:** CCI-001854 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-03-14

**Definition:** The organization defines the percentage of maximum audit record storage capacity that is to be reached, at which time the information system will provide a warning to organization-defined personnel, roles, and/or locations.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-5 (1)

---

**CCI:** CCI-001855 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-03-14

**Definition:** The information system provides a warning to organization-defined personnel, roles, and/or locations within an organization-defined time period when allocated audit record storage volume reaches an organization-defined percentage of repository maximum audit record storage capacity.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-5 (1)

---

**CCI:** CCI-000147 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-05-22

**Definition:** The organization defines the audit failure events requiring real-time alerts.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AU-5 (2)
NIST: NIST SP 800-53 Revision 4 (v4): AU-5 (2)
NIST: NIST SP 800-53A (v1): AU-5 (2).1 (i)

---

**CCI:** CCI-001856 **Status:** draft

| | | | |
|---|---|---|---|
| **Contributor:** | DISA FSO | **Published Date:** | 2013-03-14 |
| **Definition:** | The organization defines the real-time period within which the information system is to provide an alert when organization-defined audit failure events occur. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AU-5 (2) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001857 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-03-14 |
| **Definition:** | The organization defines the personnel, roles, and/or locations to receive alerts when organization-defined audit failure events occur. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AU-5 (2) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001858 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-03-14 |
| **Definition:** | The information system provides a real-time alert in an organization-defined real-time period to organization-defined personnel, roles, and/or locations when organization-defined audit failure events requiring real-time alerts occur. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AU-5 (2) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001573 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-11 |
| **Definition:** | The organization defines whether to reject or delay network traffic that exceeds organization-defined thresholds. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AU-5 (3)<br>NIST: NIST SP 800-53 Revision 4 (v4): AU-5 (3)<br>NIST: NIST SP 800-53A (v1): AU-5 (3).1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000145 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-05-20 |
| **Definition:** | The information system enforces configurable network communications traffic volume thresholds reflecting limits on auditing capacity by delaying or rejecting network traffic which exceeds the organization-defined thresholds. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AU-5 (3)<br>NIST: NIST SP 800-53 Revision 4 (v4): AU-5 (3)<br>NIST: NIST SP 800-53A (v1): AU-5 (3).1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001859 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-03-14 |
| **Definition:** | The organization defines the network communication traffic volume thresholds reflecting limits on auditing capacity, specifying when the information system will reject or delay network traffic that exceed those thresholds. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AU-5 (3) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001860 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-03-14 |
| **Definition:** | The organization defines the audit failures which, should they occur, will invoke an organization-defined system mode. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AU-5 (4) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001861 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-03-14 |
| **Definition:** | The information system invokes an organization-defined system mode, in the event of organization-defined audit failures, unless an alternate audit capability exists. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AU-5 (4) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002907 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-08-22 |
| **Definition:** | The organization defines the system mode to be invoked, such as a full system shutdown, a partial system shutdown, or a degraded operational mode with limited mission/business functionality available, in the event of organization-defined audit failures. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AU-5 (4) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000148 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-05-22 |
| **Definition:** | The organization reviews and analyzes information system audit records on an organization-defined frequency for indications of organization-defined inappropriate or unusual activity. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AU-6 a<br>NIST: NIST SP 800-53 Revision 4 (v4): AU-6 a<br>NIST: NIST SP 800-53A (v1): AU-6.1 (ii) | | |

**CCI:** CCI-000151 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-15
**Definition:** The organization defines the frequency for the review and analysis of information system audit records for organization-defined inappropriate or unusual activity.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): AU-6 a
NIST: NIST SP 800-53 Revision 4 (v4): AU-6 a
NIST: NIST SP 800-53A (v1): AU-6.1 (i)

---

**CCI:** CCI-001862 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-03-15
**Definition:** The organization defines the types of inappropriate or unusual activity to be reviewed and analyzed in the audit records.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-6 a

---

**CCI:** CCI-000149 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-05-22
**Definition:** The organization reports any findings to organization-defined personnel or roles for indications of organization-defined inappropriate or unusual activity.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): AU-6 a
NIST: NIST SP 800-53 Revision 4 (v4): AU-6 b
NIST: NIST SP 800-53A (v1): AU-6.1 (iii)

---

**CCI:** CCI-001863 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-03-15
**Definition:** The organization defines the personnel or roles to receive the reports of organization-defined inappropriate or unusual activity.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-6 b

---

**CCI:** CCI-001864 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-03-15
**Definition:** The organization employs automated mechanisms to integrate audit review and analysis to support organizational processes for investigation of and response to suspicious activities.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-6 (1)

---

**CCI:** CCI-001865 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-03-15
**Definition:** The organization employs automated mechanisms to integrate reporting processes to support organizational investigation of and response to suspicious activities.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-6 (1)

---

**CCI:** CCI-000153 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-05-22
**Definition:** The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): AU-6 (3)
NIST: NIST SP 800-53 Revision 4 (v4): AU-6 (3)
NIST: NIST SP 800-53A (v1): AU-6 (3).1

---

**CCI:** CCI-000154 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-05-22
**Definition:** The information system provides the capability to centrally review and analyze audit records from multiple components within the system.
**Type:** technical
**References:** NIST: NIST SP 800-53 (v3): AU-6 (4)
NIST: NIST SP 800-53 Revision 4 (v4): AU-6 (4)
NIST: NIST SP 800-53A (v1): AU-6 (4).1

---

**CCI:** CCI-001866 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-03-15
**Definition:** The organization defines the data/information to be collected from other sources to enhance its ability to identify inappropriate or unusual activity.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-6 (5)

---

**CCI:** CCI-001867 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-03-15
**Definition:** The organization integrates analysis of audit records with analysis of vulnerability scanning information, performance data, information system monitoring information, and/or organization-defined data/information collected from other sources to further enhance its ability to identify inappropriate or unusual activity.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-6 (5)

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001491 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-29 |
| **Definition:** | The organization correlates information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AU-6 (6)<br>NIST: NIST SP 800-53 Revision 4 (v4): AU-6 (6)<br>NIST: NIST SP 800-53A (v1): AU-6 (6).1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001868 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-03-15 |
| **Definition:** | The organization specifies the permitted actions for each information system process, role, and/or user associated with the review and analysis of audit information. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AU-6 (7) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001869 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-03-15 |
| **Definition:** | The organization specifies the permitted actions for each information system process, role, and/or user associated with the reporting of audit information. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AU-6 (7) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001870 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-03-15 |
| **Definition:** | The organization performs a full-text analysis of audited privileged commands in a physically-distinct component or subsystem of the information system, or other information system that is dedicated to that analysis. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AU-6 (8) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001871 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-03-15 |
| **Definition:** | The organization correlates information from non-technical sources with audit information to enhance organization-wide situational awareness. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AU-6 (9) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001872 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-03-15 |
| **Definition:** | The organization adjusts the level of audit review and analysis within the information system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AU-6 (10) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001873 | **Status:** | deprecated |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-03-15 |
| **Definition:** | The organization adjusts the level of audit analysis within the information system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AU-6 (10) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001874 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-03-15 |
| **Definition:** | The organization adjusts the level of audit reporting within the information system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AU-6 (10) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001875 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-03-15 |
| **Definition:** | The information system provides an audit reduction capability that supports on-demand audit review and analysis. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AU-7 a | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001876 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-03-15 |
| **Definition:** | The information system provides an audit reduction capability that supports on-demand reporting requirements. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AU-7 a | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001877 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published** | 2013-03-15 |

**Date:**

**Definition:** The information system provides an audit reduction capability that supports after-the-fact investigations of security incidents.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-7 a

---

**CCI:** CCI-001878 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-03-15

**Definition:** The information system provides a report generation capability that supports on-demand audit review and analysis.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-7 a

---

**CCI:** CCI-001879 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-03-15

**Definition:** The information system provides a report generation capability that supports on-demand reporting requirements.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-7 a

---

**CCI:** CCI-001880 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-03-15

**Definition:** The information system provides a report generation capability that supports after-the-fact investigations of security incidents.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-7 a

---

**CCI:** CCI-001881 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-03-15

**Definition:** The information system provides an audit reduction capability that does not alter original content or time ordering of audit records.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-7 b

---

**CCI:** CCI-001882 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-03-15

**Definition:** The information system provides a report generation capability that does not alter original content or time ordering of audit records.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-7 b

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000158 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-05-22 |
| **Definition:** | The information system provides the capability to process audit records for events of interest based on organization-defined audit fields within audit records. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): AU-7 (1)<br>NIST: NIST SP 800-53 Revision 4 (v4): AU-7 (1)<br>NIST: NIST SP 800-53A (v1): AU-7 (1).1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001883 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-03-15 |
| **Definition:** | The organization defines the audit fields within audit records to be processed for events of interest by the information system. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AU-7 (1) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001884 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-03-15 |
| **Definition:** | The organization defines the audit fields within audit records to be sorted for events of interest by the information system. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AU-7 (2) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001885 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-03-15 |
| **Definition:** | The organization defines the audit fields within audit records to be searched for events of interest by the information system. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AU-7 (2) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001886 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-03-15 |
| **Definition:** | The information system provides the capability to sort audit records for events of interest based on the content of organization-defined audit fields within audit records. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AU-7 (2) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001887 | **Status:** | draft |

**Contributor:** DISA FSO **Published Date:** 2013-03-15

**Definition:** The information system provides the capability to search audit records for events of interest based on the content of organization-defined audit fields within audit records.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-7 (2)

---

**CCI:** CCI-000159 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-05-22

**Definition:** The information system uses internal system clocks to generate time stamps for audit records.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AU-8
NIST: NIST SP 800-53 Revision 4 (v4): AU-8 a
NIST: NIST SP 800-53A (v1): AU-8.1

---

**CCI:** CCI-001888 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-03-15

**Definition:** The organization defines the granularity of time measurement for time stamps generated for audit records.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-8 b

---

**CCI:** CCI-001889 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-03-15

**Definition:** The information system records time stamps for audit records that meet organization-defined granularity of time measurement.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-8 b

---

**CCI:** CCI-001890 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-03-15

**Definition:** The information system records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT).

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-8 b

---

**CCI:** CCI-000161 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-05-22

**Definition:** The organization defines the frequency for the synchronization of internal information system clocks.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AU-8 (1)
NIST: NIST SP 800-53 Revision 4 (v4): AU-8 (1) (a)
NIST: NIST SP 800-53A (v1): AU-8 (1).1 (i)

---

**CCI:** CCI-001492 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-29

**Definition:** The organization defines an authoritative time source for the synchronization of internal information system clocks.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AU-8 (1)
NIST: NIST SP 800-53 Revision 4 (v4): AU-8 (1) (a)
NIST: NIST SP 800-53A (v1): AU-8 (1).1 (ii)

---

**CCI:** CCI-001891 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-03-15

**Definition:** The information system compares internal information system clocks on an organization-defined frequency with an organization-defined authoritative time source.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-8 (1) (a)

---

**CCI:** CCI-001892 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-03-15

**Definition:** The organization defines the time difference which, when exceeded, will require the information system to synchronize the internal information system clocks to the organization-defined authoritative time source.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-8 (1) (b)

---

**CCI:** CCI-002046 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-05-29

**Definition:** The information system synchronizes the internal system clocks to the authoritative time source when the time difference is greater than the organization-defined time period.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-8 (1) (b)

---

**CCI:** CCI-001893 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-03-15

**Definition:** The information system identifies a secondary authoritative time source that is located in a different geographic region than the primary authoritative time source.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-8 (2)

---

**CCI:** CCI-000162 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-05-22

**Definition:** The information system protects audit information from unauthorized access.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AU-9

NIST: NIST SP 800-53 Revision 4 (v4): AU-9

NIST: NIST SP 800-53A (v1): AU-9.1

---

**CCI:** CCI-000163 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-05-22

**Definition:** The information system protects audit information from unauthorized modification.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AU-9

NIST: NIST SP 800-53 Revision 4 (v4): AU-9

NIST: NIST SP 800-53A (v1): AU-9.1

---

**CCI:** CCI-000164 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-05-22

**Definition:** The information system protects audit information from unauthorized deletion.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AU-9

NIST: NIST SP 800-53 Revision 4 (v4): AU-9

NIST: NIST SP 800-53A (v1): AU-9.1

---

**CCI:** CCI-001493 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-29

**Definition:** The information system protects audit tools from unauthorized access.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AU-9

NIST: NIST SP 800-53 Revision 4 (v4): AU-9

NIST: NIST SP 800-53A (v1): AU-9.1

---

**CCI:** CCI-001494 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-29

**Definition:** The information system protects audit tools from unauthorized modification.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AU-9
NIST: NIST SP 800-53 Revision 4 (v4): AU-9
NIST: NIST SP 800-53A (v1): AU-9.1

---

**CCI:** CCI-001495 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-29

**Definition:** The information system protects audit tools from unauthorized deletion.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AU-9
NIST: NIST SP 800-53 Revision 4 (v4): AU-9
NIST: NIST SP 800-53A (v1): AU-9.1

---

**CCI:** CCI-000165 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-05-22

**Definition:** The information system writes audit records to hardware-enforced, write-once media.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AU-9 (1)
NIST: NIST SP 800-53 Revision 4 (v4): AU-9 (1)
NIST: NIST SP 800-53A (v1): AU-9 (1).1

---

**CCI:** CCI-001575 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2010-05-11

**Definition:** The organization defines the system or system component for storing audit records that is a different system or system component than the system or component being audited.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AU-9 (2)
NIST: NIST SP 800-53 Revision 4 (v4): AU-9 (2)
NIST: NIST SP 800-53A (v1): AU-9 (2).1 (i)

---

**CCI:** CCI-001348 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The information system backs up audit records on an organization-defined frequency onto a different system or system component than the system or component being audited.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AU-9 (2)
NIST: NIST SP 800-53 Revision 4 (v4): AU-9 (2)
NIST: NIST SP 800-53A (v1): AU-9 (2).1 (iii)

---

**CCI:** CCI-001349 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-22
**Definition:** The organization defines a frequency for backing up system audit records onto a different system or system component than the system or component being audited.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): AU-9 (2)
NIST: NIST SP 800-53 Revision 4 (v4): AU-9 (2)
NIST: NIST SP 800-53A (v1): AU-9 (2).1 (ii)

---

**CCI:** CCI-001350 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-22
**Definition:** The information system implements cryptographic mechanisms to protect the integrity of audit information.
**Type:** technical
**References:** NIST: NIST SP 800-53 (v3): AU-9 (3)
NIST: NIST SP 800-53 Revision 4 (v4): AU-9 (3)
NIST: NIST SP 800-53A (v1): AU-9 (3).1

---

**CCI:** CCI-001496 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-29
**Definition:** The information system implements cryptographic mechanisms to protect the integrity of audit tools.
**Type:** technical
**References:** NIST: NIST SP 800-53 (v3): AU-9 (3)
NIST: NIST SP 800-53 Revision 4 (v4): AU-9 (3)
NIST: NIST SP 800-53A (v1): AU-9 (3).1

---

**CCI:** CCI-001351 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-22
**Definition:** The organization authorizes access to management of audit functionality to only an organization-defined subset of privileged users.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): AU-9 (4) (a)
NIST: NIST SP 800-53 Revision 4 (v4): AU-9 (4)
NIST: NIST SP 800-53A (v1): AU-9 (4).1 (i)

---

**CCI:** CCI-001894 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-03-15
**Definition:** The organization defines the subset of privileged users who will be authorized access to the

management of audit functionality.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-9 (4)

---

**CCI:** CCI-001895 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-03-15

**Definition:** The organization defines the audit information requiring dual authorization for movement or deletion actions.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-9 (5)

---

**CCI:** CCI-001896 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-03-15

**Definition:** The organization enforces dual authorization for movement and/or deletion of organization-defined audit information.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-9 (5)

---

**CCI:** CCI-001897 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-03-15

**Definition:** The organization defines the subset of privileged users who will be authorized read-only access to audit information.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-9 (6)

---

**CCI:** CCI-001898 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-03-15

**Definition:** The organization authorizes read-only access to audit information to an organization-defined subset of privileged users.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-9 (6)

---

**CCI:** CCI-000166 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-05-22

**Definition:** The information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed organization-defined actions to be covered by non-repudiation.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AU-10
NIST: NIST SP 800-53 Revision 4 (v4): AU-10

NIST: NIST SP 800-53A (v1): AU-10.1

---

**CCI:** CCI-001899 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-03-15

**Definition:** The organization defines the actions to be covered by non-repudiation.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-10

---

**CCI:** CCI-001900 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-03-15

**Definition:** The organization defines the strength of binding to be applied to the binding of the identity of the information producer with the information.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-10 (1) (a)

---

**CCI:** CCI-001901 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-03-15

**Definition:** The information system binds the identity of the information producer with the information to an organization-defined strength of binding.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-10 (1) (a)

---

**CCI:** CCI-001902 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-03-15

**Definition:** The information system provides the means for authorized individuals to determine the identity of the producer of the information.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-10 (1) (b)

---

**CCI:** CCI-001903 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-03-15

**Definition:** The organization defines the frequency on which the information system is to validate the binding of the information producer identity to the information.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-10 (2) (a)

---

**CCI:** CCI-001904 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-03-15

**Definition:** The information system validates the binding of the information producer identity to the information at an organization-defined frequency.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-10 (2) (a)

---

**CCI:** CCI-001905

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2013-03-15

**Definition:** The organization defines the actions to be performed in the event of an error when validating the binding of the information producer identity to the information.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-10 (2) (b)

---

**CCI:** CCI-001906

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2013-03-15

**Definition:** The information system performs organization-defined actions in the event of an error when validating the binding of the information producer identity to the information.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-10 (2) (b)

---

**CCI:** CCI-001340

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2009-09-22

**Definition:** The information system maintains reviewer/releaser identity and credentials within the established chain of custody for all information reviewed or released.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AU-10 (3)
NIST: NIST SP 800-53 Revision 4 (v4): AU-10 (3)
NIST: NIST SP 800-53A (v1): AU-10 (3).1

---

**CCI:** CCI-001341

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2009-09-22

**Definition:** The information system validates the binding of the information reviewer identity to the information at the transfer or release points prior to release/transfer between organization-defined security domains.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AU-10 (4)
NIST: NIST SP 800-53 Revision 4 (v4): AU-10 (4) (a)
NIST: NIST SP 800-53A (v1): AU-10 (4).1

---

**CCI:** CCI-001907

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2013-03-15

**Definition:** The organization defines the security domains which will require the information system validate the binding of the information reviewer identity to the information at the transfer or release points prior to release/transfer.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-10 (4) (a)

---

**CCI:** CCI-001908 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-03-15

**Definition:** The organization defines the action the information system is to perform in the event of an information reviewer identity binding validation error.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-10 (4) (b)

---

**CCI:** CCI-001909 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-03-15

**Definition:** The information system performs organization-defined actions in the event of an information reviewer identity binding validation error.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-10 (4) (b)

---

**CCI:** CCI-000167 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-05-22

**Definition:** The organization retains audit records for an organization-defined time period to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AU-11
NIST: NIST SP 800-53 Revision 4 (v4): AU-11
NIST: NIST SP 800-53A (v1): AU-11.1 (iii)

---

**CCI:** CCI-000168 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-15

**Definition:** The organization defines the time period for retention of audit records, which is consistent with its records retention policy, to provide support for after-the-fact investigations of security incidents and meet regulatory and organizational information retention requirements.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AU-11
NIST: NIST SP 800-53 Revision 4 (v4): AU-11
NIST: NIST SP 800-53A (v1): AU-11.1 (i and ii)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002044 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-29 |
| **Definition:** | The organization defines measures to be employed to ensure that long-term audit records generated by the information system can be retrieved. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AU-11 (1) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002045 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-29 |
| **Definition:** | The organization employs organization-defined measures to ensure that long-term audit records generated by the information system can be retrieved. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AU-11 (1) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000169 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-05-22 |
| **Definition:** | The information system provides audit record generation capability for the auditable events defined in AU-2 a. at organization-defined information system components. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): AU-12 a<br>NIST: NIST SP 800-53 Revision 4 (v4): AU-12 a<br>NIST: NIST SP 800-53A (v1): AU-12.1 (ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001459 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-29 |
| **Definition:** | The organization defines information system components that provide audit record generation capability. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AU-12 a<br>NIST: NIST SP 800-53 Revision 4 (v4): AU-12 a<br>NIST: NIST SP 800-53A (v1): AU-12.1 (i) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000171 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-15 |
| **Definition:** | The information system allows organization-defined personnel or roles to select which auditable events are to be audited by specific components of the information system. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): AU-12 b<br>NIST: NIST SP 800-53 Revision 4 (v4): AU-12 b | | |

|  |  |  |  |
|---|---|---|---|
|  | NIST: NIST SP 800-53A (v1): AU-12.1 (iii) |  |  |

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-001910 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-03-15 |
| **Definition:** | The organization defines the personnel or roles allowed to select which auditable events are to be audited by specific components of the information system. |  |  |
| **Type:** | policy |  |  |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AU-12 b |  |  |

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-000172 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-15 |
| **Definition:** | The information system generates audit records for the events defined in AU-2 d. with the content defined in AU-3. |  |  |
| **Type:** | technical |  |  |
| **References:** | NIST: NIST SP 800-53 (v3): AU-12 c<br>NIST: NIST SP 800-53 Revision 4 (v4): AU-12 c<br>NIST: NIST SP 800-53A (v1): AU-12.1 (iv) |  |  |

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-001576 | **Status:** | deprecated |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-11 |
| **Definition:** | The information system produces a system-wide (logical or physical) audit trail of information system audit records. |  |  |
| **Type:** | technical |  |  |
| **References:** | NIST: NIST SP 800-53 (v3): AU-12 (1)<br>NIST: NIST SP 800-53 Revision 4 (v4): AU-12 (1)<br>NIST: NIST SP 800-53A (v1): AU-12 (1).1 (i) |  |  |

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-001577 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-11 |
| **Definition:** | The organization defines the information system components from which audit records are to be compiled into the system-wide audit trail. |  |  |
| **Type:** | policy |  |  |
| **References:** | NIST: NIST SP 800-53 (v3): AU-12 (1)<br>NIST: NIST SP 800-53 Revision 4 (v4): AU-12 (1)<br>NIST: NIST SP 800-53A (v1): AU-12 (1).1 (ii) |  |  |

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-000173 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-15 |
| **Definition:** | The organization defines the level of tolerance for relationship between time stamps of |  |  |

| | | | |
|---|---|---|---|
| | individual records in the audit trail that will be used for correlation. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AU-12 (1) | | |
| | NIST: NIST SP 800-53 Revision 4 (v4): AU-12 (1) | | |
| | NIST: NIST SP 800-53A (v1): AU-12 (1).1 (iv) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000174 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-05-22 |
| **Definition:** | The information system compiles audit records from organization-defined information system components into a system-wide (logical or physical) audit trail that is time-correlated to within an organization-defined level of tolerance for relationship between time stamps of individual records in the audit trail. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): AU-12 (1) | | |
| | NIST: NIST SP 800-53 Revision 4 (v4): AU-12 (1) | | |
| | NIST: NIST SP 800-53A (v1): AU-12 (1).1 (iii and v) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001353 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The information system produces a system-wide (logical or physical) audit trail composed of audit records in a standardized format. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): AU-12 (2) | | |
| | NIST: NIST SP 800-53 Revision 4 (v4): AU-12 (2) | | |
| | NIST: NIST SP 800-53A (v1): AU-12 (2).1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001911 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-03-15 |
| **Definition:** | The organization defines the selectable event criteria to be used as the basis for changes to the auditing to be performed on organization-defined information system components, by organization-defined individuals or roles, within organization-defined time thresholds. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AU-12 (3) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001912 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-03-15 |
| **Definition:** | The organization defines the time thresholds for organization-defined individuals or roles to change the auditing to be performed based on organization-defined selectable event criteria. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): AU-12 (3) | | |

**CCI:** CCI-001913 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-03-15
**Definition:** The organization defines the individuals or roles that are to be provided the capability to change the auditing to be performed based on organization-defined selectable event criteria, within organization-defined time thresholds.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-12 (3)

---

**CCI:** CCI-001914 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-03-15
**Definition:** The information system provides the capability for organization-defined individuals or roles to change the auditing to be performed on organization-defined information system components based on organization-defined selectable event criteria within organization-defined time thresholds.
**Type:** technical
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-12 (3)

---

**CCI:** CCI-002047 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-05-29
**Definition:** The organization defines the information system components on which the auditing that is to be performed can be changed by organization-defined individuals or roles.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-12 (3)

---

**CCI:** CCI-001460 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-29
**Definition:** The organization monitors organization-defined open source information and/or information sites per organization-defined frequency for evidence of unauthorized exfiltration or disclosure of organizational information.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): AU-13
NIST: NIST SP 800-53 Revision 4 (v4): AU-13
NIST: NIST SP 800-53A (v1): AU-13.1 (ii)

---

**CCI:** CCI-001461 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-29
**Definition:** The organization defines a frequency for monitoring open source information and/or information sites for evidence of unauthorized exfiltration or disclosure of organizational information.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AU-13<br>
NIST: NIST SP 800-53 Revision 4 (v4): AU-13<br>
NIST: NIST SP 800-53A (v1): AU-13.1 (i)

---

**CCI:** CCI-001915

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2013-03-15

**Definition:** The organization defines the open source information and/or information sites to be monitored for evidence of unauthorized exfiltration or disclosure of organizational information.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-13

---

**CCI:** CCI-001916

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2013-03-15

**Definition:** The organization employs automated mechanisms to determine if organizational information has been disclosed in an unauthorized manner.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-13 (1)

---

**CCI:** CCI-001917

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2013-03-15

**Definition:** The organization defines the frequency for reviewing the open source information sites being monitored.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-13 (2)

---

**CCI:** CCI-001918

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2013-03-15

**Definition:** The organization reviews the open source information sites being monitored per organization-defined frequency.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-13 (2)

---

**CCI:** CCI-001919

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2013-03-15

**Definition:** The information system provides the capability for authorized users to select a user session to capture/record or view/hear.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-14

---

**CCI:** CCI-001464 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-29

**Definition:** The information system initiates session audits at system start-up.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AU-14 (1)
NIST: NIST SP 800-53 Revision 4 (v4): AU-14 (1)
NIST: NIST SP 800-53A (v1): AU-14 (1).1

---

**CCI:** CCI-001462 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-29

**Definition:** The information system provides the capability for authorized users to capture/record and log content related to a user session.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AU-14 a
NIST: NIST SP 800-53 Revision 4 (v4): AU-14 (2)
NIST: NIST SP 800-53A (v1): AU-14.1 (i)

---

**CCI:** CCI-001920 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-03-15

**Definition:** The information system provides the capability for authorized users to remotely view/hear all content related to an established user session in real time.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-14 (3)

---

**CCI:** CCI-001921 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-03-15

**Definition:** The organization defines the alternative audit functionality to be provided in the event of a failure in the primary audit capability.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-15

---

**CCI:** CCI-001922 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-03-15

**Definition:** The organization provides an alternative audit capability in the event of a failure in primary audit capability that provides organization-defined alternative audit functionality.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-15

---

**CCI:** CCI-001923 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-03-15
**Definition:** The organization defines the audit information to be coordinated among external organizations when audit information is transmitted across organizational boundaries.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-16

---

**CCI:** CCI-001924 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-03-15
**Definition:** The organization defines the methods to be employed when coordinating audit information among external organizations when audit information is transmitted across organizational boundaries.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-16

---

**CCI:** CCI-001925 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-03-15
**Definition:** The organization employs organization-defined methods for coordinating organization-defined audit information among external organizations when audit information is transmitted across organizational boundaries.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-16

---

**CCI:** CCI-001926 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-03-15
**Definition:** The organization requires that the identity of individuals be preserved in cross-organizational audit trails.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-16 (1)

---

**CCI:** CCI-001927 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-03-15
**Definition:** The organization defines the organizations that will be provided cross-organizational audit information.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-16 (2)

---

**CCI:** CCI-001928 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-03-15

**Definition:** The organization defines the cross-organizational sharing agreements to be established with organization-defined organizations authorized to be provided cross-organizational sharing of audit information.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-16 (2)

---

**CCI:** CCI-001929 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-03-15

**Definition:** The organization provides cross-organizational audit information to organization-defined organizations based on organization-defined cross organizational sharing agreements.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): AU-16 (2)

---

**CCI:** CCI-000239 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-15

**Definition:** The organization develops and documents a security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CA-1 a
NIST: NIST SP 800-53 Revision 4 (v4): CA-1 a 1
NIST: NIST SP 800-53A (v1): CA-1.1 (i and ii)

---

**CCI:** CCI-000240 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-15

**Definition:** The organization disseminates to organization-defined personnel or roles a security assessment and authorization policy.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CA-1 a
NIST: NIST SP 800-53 Revision 4 (v4): CA-1 a 1
NIST: NIST SP 800-53 Revision 4 (v4): CA-1 a 1
NIST: NIST SP 800-53A (v1): CA-1.1 (iii)

---

**CCI:** CCI-000242 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-15

**Definition:** The organization develops and documents procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CA-1 b
NIST: NIST SP 800-53 Revision 4 (v4): CA-1 a 2

NIST: NIST SP 800-53A (v1): CA-1.1 (iv and v)

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000243 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-15 |
| **Definition:** | The organization disseminates to organization-defined personnel or roles procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CA-1 b<br>NIST: NIST SP 800-53 Revision 4 (v4): CA-1 a 2<br>NIST: NIST SP 800-53A (v1): CA-1.1 (vi) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002060 | **Status:** | deprecated |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-21 |
| **Definition:** | The organization develops and documents a security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CA-1 a 1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002061 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-21 |
| **Definition:** | The organization defines the personnel or roles to whom security assessment and authorization policy is to be disseminated. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CA-1 a 1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002062 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-21 |
| **Definition:** | The organization defines the personnel or roles to whom the security assessment and authorization procedures are to be disseminated. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CA-1 a 2 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001578 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-11 |
| **Definition:** | The organization defines the frequency to review and update the current security assessment and authorization procedures. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CA-1 b | | |

NIST: NIST SP 800-53 Revision 4 (v4): CA-1 b 2
NIST: NIST SP 800-53A (v1): CA-1.2 (iii)

---

**CCI:** CCI-000238 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-15
**Definition:** The organization defines the frequency to review and update the current security assessment and authorization policy.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CA-1
NIST: NIST SP 800-53 Revision 4 (v4): CA-1 b 1
NIST: NIST SP 800-53A (v1): CA-1.2 (i)

---

**CCI:** CCI-000241 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-15
**Definition:** The organization reviews and updates the current security assessment and authorization policy in accordance with organization-defined frequency.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CA-1 a
NIST: NIST SP 800-53 Revision 4 (v4): CA-1 b 1
NIST: NIST SP 800-53A (v1): CA-1.2 (ii)

---

**CCI:** CCI-000244 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-15
**Definition:** The organization reviews and updates the current security assessment and authorization procedures in accordance with organization-defined frequency.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CA-1 b
NIST: NIST SP 800-53 Revision 4 (v4): CA-1 b 2
NIST: NIST SP 800-53A (v1): CA-1.2 (iv)

---

**CCI:** CCI-000245 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-15
**Definition:** The organization develops a security assessment plan for the information system and its environment of operation.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CA-2 a
NIST: NIST SP 800-53 Revision 4 (v4): CA-2 a
NIST: NIST SP 800-53A (v1): CA-2.1 (i)

---

**CCI:** CCI-000246 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-15

**Definition:** The organization's security assessment plan describes the security controls and control enhancements under assessment.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CA-2 a
NIST: NIST SP 800-53 Revision 4 (v4): CA-2 a 1
NIST: NIST SP 800-53A (v1): CA-2.1 (ii)

---

**CCI:** CCI-000247 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-15

**Definition:** The organization's security assessment plan describes assessment procedures to be used to determine security control effectiveness.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CA-2 a
NIST: NIST SP 800-53 Revision 4 (v4): CA-2 a 2
NIST: NIST SP 800-53A (v1): CA-2.1 (ii)

---

**CCI:** CCI-000248 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-15

**Definition:** The organization's security assessment plan describes assessment environment.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CA-2 a
NIST: NIST SP 800-53 Revision 4 (v4): CA-2 a 3
NIST: NIST SP 800-53A (v1): CA-2.1 (ii)

---

**CCI:** CCI-002070 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-21

**Definition:** The organization's security assessment plan describes the assessment team, and assessment roles and responsibilities.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CA-2 a 3

---

**CCI:** CCI-000251 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-15

**Definition:** The organization assesses, on an organization-defined frequency, the security controls in the information system and its environment of operation to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CA-2 b
NIST: NIST SP 800-53 Revision 4 (v4): CA-2 b
NIST: NIST SP 800-53A (v1): CA-2.2 (ii)

---

**CCI:** CCI-000252 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-15
**Definition:** The organization defines the frequency on which the security controls in the information system and its environment of operation are assessed.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CA-2 b
NIST: NIST SP 800-53 Revision 4 (v4): CA-2 b
NIST: NIST SP 800-53A (v1): CA-2.2 (i)

---

**CCI:** CCI-000253 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-15
**Definition:** The organization produces a security assessment report that documents the results of the assessment against the information system and its environment of operation.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CA-2 c
NIST: NIST SP 800-53 Revision 4 (v4): CA-2 c
NIST: NIST SP 800-53A (v1): CA-2.2 (iii)

---

**CCI:** CCI-000254 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-15
**Definition:** The organization provides the results of the security control assessment against the information system and its environment of operation to organization-defined individuals or roles.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CA-2 d
NIST: NIST SP 800-53 Revision 4 (v4): CA-2 d
NIST: NIST SP 800-53A (v1): CA-2.2 (iv)

---

**CCI:** CCI-002071 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-06-21
**Definition:** The organization defines the individuals or roles to whom the results of the security control assessment are to be provided.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): CA-2 d

---

**CCI:** CCI-000255 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-15

**Definition:** The organization employs assessors or assessment teams with an organization-defined level of independence to conduct security control assessments of organizational information systems.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CA-2 (1)
NIST: NIST SP 800-53 Revision 4 (v4): CA-2 (1)
NIST: NIST SP 800-53A (v1): CA-2 (1).1

---

**CCI:** CCI-002063 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-21

**Definition:** The organization defines the level of independence for assessors or assessment teams to conduct security control assessments of organizational information systems.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CA-2 (1)

---

**CCI:** CCI-000256 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-15

**Definition:** The organization includes, as part of security control assessments announced or unannounced, one or more of the following: in-depth monitoring; vulnerability scanning; malicious user testing; insider threat assessment; performance/load testing; and organization-defined other forms of security assessment on an organization-defined frequency.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CA-2 (2)
NIST: NIST SP 800-53 Revision 4 (v4): CA-2 (2)
NIST: NIST SP 800-53A (v1): CA-2 (2).1 (i)

---

**CCI:** CCI-001582 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2010-05-11

**Definition:** The organization defines other forms of security assessments other than in-depth monitoring; vulnerability scanning; malicious user testing; insider threat assessment; and performance/load testing that should be included as part of security control assessments.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CA-7 (2)
NIST: NIST SP 800-53 Revision 4 (v4): CA-2 (2)
NIST: NIST SP 800-53A (v1): CA-7 (2).1 (i)

---

**CCI:** CCI-001583 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2010-05-11

**Definition:** The organization selects announced or unannounced assessments for each form of security control assessment.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CA-7 (2)
NIST: NIST SP 800-53 Revision 4 (v4): CA-2 (2)
NIST: NIST SP 800-53A (v1): CA-7 (2).1 (i)

---

**CCI:** CCI-001681 **Status:** deprecated

**Contributor:** DISA FSO **Published Date:** 2011-04-26

**Definition:** The organization defines the frequency at which each form of security control assessment should be conducted.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CA-7 (2)
NIST: NIST SP 800-53 Revision 4 (v4): CA-2 (2)
NIST: NIST SP 800-53A (v1): CA-7(2).1 (i)

---

**CCI:** CCI-002064 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-21

**Definition:** The organization selects one or more security assessment techniques to be conducted.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CA-2 (2)

---

**CCI:** CCI-002065 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-21

**Definition:** The organization defines the frequency at which to conduct security control assessments.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CA-2 (2)

---

**CCI:** CCI-002066 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-21

**Definition:** The organization accepts the results of an assessment of the organization-defined information system performed by an organization-defined external organization when the assessment meets organization-defined requirements.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CA-2 (3)

---

**CCI:** CCI-002067 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-21

**Definition:** The organization defines the information systems for which they will accept the results of an

| | | | |
|---|---|---|---|
| | assessment performed by an external organization. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CA-2 (3) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002068 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-21 |
| **Definition:** | The organization defines the external organizations from which assessment results for organization-defined information systems will be accepted. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CA-2 (3) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002069 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-21 |
| **Definition:** | The organization defines the requirements the assessments for organization-defined information systems from organization-defined external organizations must meet. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CA-2 (3) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000257 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-15 |
| **Definition:** | The organization authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CA-3 a<br>NIST: NIST SP 800-53 Revision 4 (v4): CA-3 a<br>NIST: NIST SP 800-53A (v1): CA-3.1 (ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000258 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-15 |
| **Definition:** | The organization documents, for each interconnection, the interface characteristics. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CA-3 b<br>NIST: NIST SP 800-53 Revision 4 (v4): CA-3 b<br>NIST: NIST SP 800-53A (v1): CA-3.1 (iii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000259 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-15 |
| **Definition:** | The organization documents, for each interconnection, the security requirements. | | |
| **Type:** | policy | | |

**References:** NIST: NIST SP 800-53 (v3): CA-3 b
NIST: NIST SP 800-53 Revision 4 (v4): CA-3 b
NIST: NIST SP 800-53A (v1): CA-3.1 (iii)

---

**CCI:** CCI-000260
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2009-09-15
**Definition:** The organization documents, for each interconnection, the nature of the information communicated.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CA-3 b
NIST: NIST SP 800-53 Revision 4 (v4): CA-3 b
NIST: NIST SP 800-53A (v1): CA-3.1 (iii)

---

**CCI:** CCI-002083
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2013-06-21
**Definition:** The organization reviews and updates Interconnection Security Agreements on an organization-defined frequency.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): CA-3 c

---

**CCI:** CCI-002084
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2013-06-21
**Definition:** The organization defines the frequency at which reviews and updates to the Interconnection Security Agreements must be conducted.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): CA-3 c

---

**CCI:** CCI-000262
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2009-09-15
**Definition:** The organization prohibits the direct connection of an organization-defined unclassified, national security system to an external network without the use of an organization-defined boundary protection device.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CA-3 (1)
NIST: NIST SP 800-53 Revision 4 (v4): CA-3 (1)
NIST: NIST SP 800-53A (v1): CA-3 (1).1

---

**CCI:** CCI-002072
**Status:** draft
**Contributor:** DISA FSP
**Published Date:** 2013-06-21

| | | | |
|---|---|---|---|
| **Definition:** | The organization defines the unclassified, national security systems that are prohibited from directly connecting to an external network without the use of an organization-defined boundary protection device. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CA-3 (1) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002073 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-21 |
| **Definition:** | The organization defines the boundary protection device to be used to connect organization-defined unclassified, national security systems to an external network. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CA-3 (1) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000263 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-15 |
| **Definition:** | The organization prohibits the direct connection of a classified, national security system to an external network without the use of organization-defined boundary protection device. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CA-3 (2)<br>NIST: NIST SP 800-53 Revision 4 (v4): CA-3 (2)<br>NIST: NIST SP 800-53A (v1): CA-3 (2).1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002074 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-21 |
| **Definition:** | The organization defines the boundary protection device to be used for the direct connection of classified, national security system to an external network. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CA-3 (2) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002075 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-21 |
| **Definition:** | The organization prohibits the direct connection of an organization-defined unclassified, non-national security system to an external network without the use of organization-defined boundary protection device. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CA-3 (3) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002076 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-21 |
| **Definition:** | The organization defines the unclassified, non-national security system that is prohibited | | |

from directly connecting to an external network without the use of an organization-defined boundary protection device.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CA-3 (3)

---

**CCI:** CCI-002077 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-21

**Definition:** The organization defines the boundary protection device to be used to directly connect an organization-defined unclassified, non-national security system to an external network.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CA-3 (3)

---

**CCI:** CCI-002078 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-21

**Definition:** The organization prohibits the direct connection of an organization-defined information system to a public network.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CA-3 (4)

---

**CCI:** CCI-002079 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-21

**Definition:** The organization defines the information system that is prohibited from directly connecting to a public network.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CA-3 (4)

---

**CCI:** CCI-002080 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-21

**Definition:** The organization employs either an allow-all, deny-by-exception or a deny-all, permit-by-exception policy for allowing organization-defined information systems to connect to external information systems.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CA-3 (5)

---

**CCI:** CCI-002081 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-21

**Definition:** The organization defines the information systems that employ either an allow-all, deny-by-exception or a deny-all, permit-by-exception policy for allowing connections to external information systems.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CA-3 (5)

---

**CCI:** CCI-002082 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-06-21
**Definition:** The organization selects either an allow-all, deny-by-exception or a deny-all, permit-by-exception policy for allowing organization-defined information systems to connect to external information systems.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): CA-3 (5)

---

**CCI:** CCI-000264 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-15
**Definition:** The organization develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CA-5 a
NIST: NIST SP 800-53 Revision 4 (v4): CA-5 a
NIST: NIST SP 800-53A (v1): CA-5-1 (i) and (ii)

---

**CCI:** CCI-000265 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-15
**Definition:** The organization defines the frequency with which to update the existing plan of action and milestones for the information system.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CA-5 b
NIST: NIST SP 800-53 Revision 4 (v4): CA-5 b
NIST: NIST SP 800-53A (v1): CA-5-1 (iii)

---

**CCI:** CCI-000266 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-15
**Definition:** The organization updates, on an organization-defined frequency, the existing plan of action and milestones for the information system based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CA-5 b
NIST: NIST SP 800-53 Revision 4 (v4): CA-5 b
NIST: NIST SP 800-53A (v1): CA-5-1 (iv)

---

**CCI:** CCI-000267 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-15

**Definition:** The organization employs automated mechanisms to help ensure the plan of action and milestones for the information system is accurate.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CA-5 (1)
NIST: NIST SP 800-53 Revision 4 (v4): CA-5 (1)
NIST: NIST SP 800-53A (v1): CA-5 (1).1

---

**CCI:** CCI-000268 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-15

**Definition:** The organization employs automated mechanisms to help ensure the plan of action and milestones for the information system is up to date.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CA-5 (1)
NIST: NIST SP 800-53 Revision 4 (v4): CA-5 (1)
NIST: NIST SP 800-53A (v1): CA-5 (1).1

---

**CCI:** CCI-000269 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-15

**Definition:** The organization employs automated mechanisms to help ensure the plan of action and milestones for the information system is readily available.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CA-5 (1)
NIST: NIST SP 800-53 Revision 4 (v4): CA-5 (1)
NIST: NIST SP 800-53A (v1): CA-5 (1).1

---

**CCI:** CCI-000270 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-15

**Definition:** The organization assigns a senior-level executive or manager as the authorizing official for the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CA-6 a
NIST: NIST SP 800-53 Revision 4 (v4): CA-6 a
NIST: NIST SP 800-53A (v1): CA-6.1 (i)

---

**CCI:** CCI-000271 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-15

**Definition:** The organization ensures the authorizing official authorizes the information system for processing before commencing operations.

| | | | |
|---|---|---|---|
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CA-6 b<br>NIST: NIST SP 800-53 Revision 4 (v4): CA-6 b<br>NIST: NIST SP 800-53A (v1): CA-6.1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000272 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-15 |
| **Definition:** | The organization updates the security authorization on an organization-defined frequency. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CA-6 c<br>NIST: NIST SP 800-53 Revision 4 (v4): CA-6 c<br>NIST: NIST SP 800-53A (v1): CA-6.1 (iv) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000273 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-15 |
| **Definition:** | The organization defines the frequency with which to update the security authorization. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CA-6 c<br>NIST: NIST SP 800-53 Revision 4 (v4): CA-6 c<br>NIST: NIST SP 800-53A (v1): CA-6.1 (iii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000274 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-15 |
| **Definition:** | The organization develops a continuous monitoring strategy. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CA-7<br>NIST: NIST SP 800-53 Revision 4 (v4): CA-7<br>NIST: NIST SP 800-53A (v1): CA-7.1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002087 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-21 |
| **Definition:** | The organization establishes and defines the metrics to be monitored for the continuous monitoring program. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CA-7 a | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002088 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-21 |
| **Definition:** | The organization establishes and defines the frequencies for continuous monitoring. | | |

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CA-7 b

---

**CCI:** CCI-002089 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-21

**Definition:** The organization establishes and defines the frequencies for assessments supporting continuous monitoring.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CA-7 b

---

**CCI:** CCI-000279 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-15

**Definition:** The organization implements a continuous monitoring program that includes ongoing security control assessments in accordance with the organizational continuous monitoring strategy.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CA-7 c
NIST: NIST SP 800-53 Revision 4 (v4): CA-7 c
NIST: NIST SP 800-53A (v1): CA-7.1 (iv)

---

**CCI:** CCI-002090 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-21

**Definition:** The organization implements a continuous monitoring program that includes ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CA-7 d

---

**CCI:** CCI-002091 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-21

**Definition:** The organization implements a continuous monitoring program that includes correlation and analysis of security-related information generated by assessments and monitoring.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CA-7 e

---

**CCI:** CCI-002092 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-21

**Definition:** The organization implements a continuous monitoring program that includes response actions to address results of the analysis of security-related information.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CA-7 f

---

**CCI:** CCI-001581 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2010-05-11

**Definition:** The organization defines personnel or roles to whom the security status of the organization and the information system should be reported.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CA-7 a
NIST: NIST SP 800-53 Revision 4 (v4): CA-7 g
NIST: NIST SP 800-53A (v1): CA-7.1 (iii)

---

**CCI:** CCI-000280 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-15

**Definition:** The organization implements a continuous monitoring program that includes reporting the security status of the organization and the information system to organization-defined personnel or roles on an organization-defined frequency.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CA-7 d
NIST: NIST SP 800-53 Revision 4 (v4): CA-7 g
NIST: NIST SP 800-53A (v1): CA-7.1 (iv)

---

**CCI:** CCI-000281 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-15

**Definition:** The organization defines the frequency with which to report the security status of the organization and the information system to organization-defined personnel or roles.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CA-7 d
NIST: NIST SP 800-53 Revision 4 (v4): CA-7 g
NIST: NIST SP 800-53A (v1): CA-7.1 (ii)

---

**CCI:** CCI-000282 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-15

**Definition:** The organization employs assessors or assessment teams with an organization-defined level of independence to monitor the security controls in the information system on an ongoing basis.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CA-7 (1)
NIST: NIST SP 800-53 Revision 4 (v4): CA-7 (1)
NIST: NIST SP 800-53A (v1): CA-7 (1).1

---

**CCI:** CCI-002085 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-06-21
**Definition:** The organization defines the level of independence the assessors or assessment teams must have to monitor the security controls in the information system on an ongoing basis.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): CA-7 (1)

---

**CCI:** CCI-002086 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-06-21
**Definition:** The organization employs trend analyses to determine if security control implementations, the frequency of continuous monitoring activities, and/or the types of activities used in the continuous monitoring process need to be modified based on empirical data.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): CA-7 (3)

---

**CCI:** CCI-002093 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-06-21
**Definition:** The organization conducts penetration testing in accordance with organization-defined frequency on organization-defined information systems or system components.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): CA-8

---

**CCI:** CCI-002094 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-06-21
**Definition:** The organization defines the frequency for conducting penetration testing on organization-defined information systems or system components.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): CA-8

---

**CCI:** CCI-002095 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-06-21
**Definition:** The organization defines the information systems or system components on which penetration testing will be conducted.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): CA-8

---

**CCI:** CCI-002096 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-06-21
**Definition:** The organization employs an independent penetration agent or penetration team to perform

| | | | |
|---|---|---|---|
| | penetration testing on the information system or system components. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CA-8 (1) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002097 | **Status:** | draft |
| **Contributor:** | DISA FSP | **Published Date:** | 2013-06-21 |
| **Definition:** | The organization defines red team exercises to simulate attempts by adversaries to compromise organizational information systems. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CA-8 (2) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002098 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-21 |
| **Definition:** | The organization defines rules of engagement for red team exercises to simulate attempts by adversaries to compromise organizational information systems. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CA-8 (2) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002099 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-21 |
| **Definition:** | The organization employs organization-defined red team exercises to simulate attempts by adversaries to compromise organizational information systems in accordance with organization-defined rules of engagement. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CA-8 (2) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002101 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-21 |
| **Definition:** | The organization authorizes internal connections of organization-defined information system components or classes of components to the information system. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CA-9 (a) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002102 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-21 |
| **Definition:** | The organization defines the information system components or classes of components that are authorized internal connections to the information system. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CA-9 (a) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002103 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-21 |
| **Definition:** | The organization documents, for each internal connection, the interface characteristics. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CA-9 (b) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002104 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-21 |
| **Definition:** | The organization documents, for each internal connection, the security requirements. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CA-9 (b) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002105 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-21 |
| **Definition:** | The organization documents, for each internal connection, the nature of the information communicated. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CA-9 (b) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002100 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-21 |
| **Definition:** | The information system performs security compliance checks on constituent components prior to the establishment of the internal connection. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CA-9 (1) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000287 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |
| **Definition:** | The organization develops and documents a configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CM-1 a<br>NIST: NIST SP 800-53 Revision 4 (v4): CM-1 a 1<br>NIST: NIST SP 800-53A (v1): CM-1.1 (i) (ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000290 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |

**Definition:** The organization develops and documents procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-1 b<br>
NIST: NIST SP 800-53 Revision 4 (v4): CM-1 a 2<br>
NIST: NIST SP 800-53A (v1): CM-1.1 (iv) (v)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001820 | **Status:** | deprecated |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-03-01 |

**Definition:** The organization documents a configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-1 a 1

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001821 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-03-01 |

**Definition:** The organization defines the organizational personnel or roles to whom the configuration management policy is to be disseminated.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-1 a 1

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001822 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-03-01 |

**Definition:** The organization disseminates the configuration management policy to organization-defined personnel or roles.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-1 a 1

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001823 | **Status:** | deprecated |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-03-01 |

**Definition:** The organization documents the procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-1 a 2

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001824 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-03-01 |

**Definition:** The organization defines the organizational personnel or roles to whom the configuration management procedures are to be disseminated.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-1 a 2

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-001825 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-03-01 |

**Definition:** The organization disseminates to organization-defined personnel or roles the procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-1 a 2

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-001584 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-11 |

**Definition:** The organization defines the frequency with which to review and update configuration management procedures.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-1
NIST: NIST SP 800-53 Revision 4 (v4): CM-1 b 2
NIST: NIST SP 800-53A (v1): CM-1.2 (iii)

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-000286 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |

**Definition:** The organization defines a frequency with which to review and update the configuration management policies.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-1
NIST: NIST SP 800-53 Revision 4 (v4): CM-1 b 1
NIST: NIST SP 800-53A (v1): CM-1.2 (i)

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-000289 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |

**Definition:** The organization reviews and updates, on an organization-defined frequency, the configuration management policy.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-1 a
NIST: NIST SP 800-53 Revision 4 (v4): CM-1 b 1
NIST: NIST SP 800-53A (v1): CM-1.2 (ii)

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-000292 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published** | 2009-09-17 |

**Date:**

**Definition:** The organization reviews and updates, on an organization-defined frequency, the procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-1 b
NIST: NIST SP 800-53 Revision 4 (v4): CM-1 b 2
NIST: NIST SP 800-53A (v1): CM-1.2 (iv)

---

**CCI:** CCI-000293 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-17

**Definition:** The organization develops a current baseline configuration of the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-2
NIST: NIST SP 800-53 Revision 4 (v4): CM-2
NIST: NIST SP 800-53A (v1): CM-2.1 (i)

---

**CCI:** CCI-000294 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-17

**Definition:** The organization documents a baseline configuration of the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-2
NIST: NIST SP 800-53 Revision 4 (v4): CM-2
NIST: NIST SP 800-53A (v1): CM-2.1 (i)

---

**CCI:** CCI-000295 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-17

**Definition:** The organization maintains, under configuration control, a current baseline configuration of the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-2
NIST: NIST SP 800-53 Revision 4 (v4): CM-2
NIST: NIST SP 800-53A (v1): CM-2.1 (ii)

---

**CCI:** CCI-000296 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-17

**Definition:** The organization reviews and updates the baseline configuration of the information system at an organization-defined frequency.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-2 (1) (a)

NIST: NIST SP 800-53 Revision 4 (v4): CM-2 (1) (a)
NIST: NIST SP 800-53A (v1): CM-2 (1).1 (ii)

---

**CCI:** CCI-001497 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-29
**Definition:** The organization defines a frequency for the reviews and updates to the baseline configuration of the information system.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CM-2 (1) (a)
NIST: NIST SP 800-53 Revision 4 (v4): CM-2 (1) (a)
NIST: NIST SP 800-53A (v1): CM-2 (1).1 (i)

---

**CCI:** CCI-001585 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2010-05-12
**Definition:** The organization defines the circumstances that require reviews and updates to the baseline configuration of the information system.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CM-2 (1) (b)
NIST: NIST SP 800-53 Revision 4 (v4): CM-2 (1) (b)
NIST: NIST SP 800-53A (v1): CM-2 (1).1 (i)

---

**CCI:** CCI-000297 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-17
**Definition:** The organization reviews and updates the baseline configuration of the information system when required due to organization-defined circumstances.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CM-2 (1) (b)
NIST: NIST SP 800-53 Revision 4 (v4): CM-2 (1) (b)
NIST: NIST SP 800-53A (v1): CM-2 (1).1 (ii)

---

**CCI:** CCI-000298 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-17
**Definition:** The organization reviews and updates the baseline configuration of the information system as an integral part of information system component installations.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CM-2 (1) (c)
NIST: NIST SP 800-53 Revision 4 (v4): CM-2 (1) (c)
NIST: NIST SP 800-53A (v1): CM-2 (1).1 (ii)

---

**CCI:** CCI-000299 **Status:** draft

| | | | |
|---|---|---|---|
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |
| **Definition:** | The organization reviews and updates the baseline configuration of the information system as an integral part of information system component upgrades. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CM-2 (1) (c)<br>NIST: NIST SP 800-53 Revision 4 (v4): CM-2 (1) (c)<br>NIST: NIST SP 800-53A (v1): CM-2 (1).1 (ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000300 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |
| **Definition:** | The organization employs automated mechanisms to maintain a complete baseline configuration of the information system. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CM-2 (2)<br>NIST: NIST SP 800-53 Revision 4 (v4): CM-2 (2)<br>NIST: NIST SP 800-53A (v1): CM-2 (2).1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000301 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |
| **Definition:** | The organization employs automated mechanisms to maintain an up-to-date baseline configuration of the information system. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CM-2 (2)<br>NIST: NIST SP 800-53 Revision 4 (v4): CM-2 (2)<br>NIST: NIST SP 800-53A (v1): CM-2 (2).1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000302 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |
| **Definition:** | The organization employs automated mechanisms to maintain an accurate baseline configuration of the information system. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CM-2 (2)<br>NIST: NIST SP 800-53 Revision 4 (v4): CM-2 (2)<br>NIST: NIST SP 800-53A (v1): CM-2 (2).1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000303 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |
| **Definition:** | The organization employs automated mechanisms to maintain a readily available baseline configuration of the information system. | | |

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-2 (2)
NIST: NIST SP 800-53 Revision 4 (v4): CM-2 (2)
NIST: NIST SP 800-53A (v1): CM-2 (2).1

---

**CCI:** CCI-000304 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-17

**Definition:** The organization retains organization-defined previous versions of baseline configurations of the information system to support rollback.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-2 (3)
NIST: NIST SP 800-53 Revision 4 (v4): CM-2 (3)
NIST: NIST SP 800-53A (v1): CM-2 (3).1

---

**CCI:** CCI-001736 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-02-28

**Definition:** The organization defines the previous versions of the baseline configuration of the information system required to support rollback.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-2 (3)

---

**CCI:** CCI-000311 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-17

**Definition:** The organization maintains a baseline configuration for information system development environments that is managed separately from the operational baseline configuration.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-2 (6)
NIST: NIST SP 800-53 Revision 4 (v4): CM-2 (6)
NIST: NIST SP 800-53A (v1): CM-2 (6).1

---

**CCI:** CCI-000312 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-17

**Definition:** The organization maintains a baseline configuration for information system test environments that is managed separately from the operational baseline configuration.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-2 (6)
NIST: NIST SP 800-53 Revision 4 (v4): CM-2 (6)
NIST: NIST SP 800-53A (v1): CM-2 (6).1

---

**CCI:** CCI-001737 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-02-28

**Definition:** The organization defines the information systems, system components, or devices that are to have organization-defined configurations applied when located in areas of significant risk.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-2 (7) (a)

---

**CCI:** CCI-001738 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-02-28

**Definition:** The organization defines the security configurations to be implemented on information systems, system components, or devices when they are located in areas of significant risk.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-2 (7) (a)

---

**CCI:** CCI-001739 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-02-28

**Definition:** The organization issues organization-defined information systems, system components, or devices with organization-defined configurations to individuals traveling to locations the organization deems to be of significant risk.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-2 (7) (a)

---

**CCI:** CCI-001815 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-03-01

**Definition:** The organization defines the security safeguards to be applied to devices when they return from areas of significant risk.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-2 (7) (b)

---

**CCI:** CCI-001816 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-03-01

**Definition:** The organization applies organization-defined security safeguards to devices when individuals return from areas of significant risk.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-2 (7) (b)

---

**CCI:** CCI-000313 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-17

**Definition:** The organization determines the types of changes to the information system that are configuration controlled.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-3 a
NIST: NIST SP 800-53 Revision 4 (v4): CM-3 a
NIST: NIST SP 800-53A (v1): CM-3.1 (i)

---

**CCI:** CCI-000314 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-17

**Definition:** The organization approves or disapproves configuration-controlled changes to the information system, with explicit consideration for security impact analysis.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-3 b
NIST: NIST SP 800-53 Revision 4 (v4): CM-3 b
NIST: NIST SP 800-53A (v1): CM-3.1 (ii)

---

**CCI:** CCI-001740 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-02-28

**Definition:** The organization reviews proposed configuration-controlled changes to the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-3 b

---

**CCI:** CCI-001741 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-02-28

**Definition:** The organization documents configuration change decisions associated with the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-3 c

---

**CCI:** CCI-001819 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-03-01

**Definition:** The organization implements approved configuration-controlled changes to the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-3 d

---

**CCI:** CCI-000316 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-17

**Definition:** The organization retains records of configuration-controlled changes to the information system for an organization-defined time period.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-3 d
NIST: NIST SP 800-53 Revision 4 (v4): CM-3 e
NIST: NIST SP 800-53A (v1): CM-3.1 (iv)

---

**CCI:** CCI-002056 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-06-11

**Definition:** The organization defines the time period the records of configuration-controlled changes are to be retained.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-3 e

---

**CCI:** CCI-000318 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-17

**Definition:** The organization audits and reviews activities associated with configuration-controlled changes to the system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-3 e
NIST: NIST SP 800-53 Revision 4 (v4): CM-3 f
NIST: NIST SP 800-53A (v1): CM-3.1 (v)

---

**CCI:** CCI-001586 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2010-05-12

**Definition:** The organization defines the configuration change control element (e.g., committee, board) responsible for coordinating and providing oversight for configuration change control activities.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-3 f
NIST: NIST SP 800-53 Revision 4 (v4): CM-3 g
NIST: NIST SP 800-53A (v1): CM-3.1 (vi)

---

**CCI:** CCI-000319 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-17

**Definition:** The organization coordinates and provides oversight for configuration change control activities through an organization-defined configuration change control element (e.g., committee, board) that convenes at the organization-defined frequency and/or for any organization-defined configuration change conditions.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-3 f
NIST: NIST SP 800-53 Revision 4 (v4): CM-3 g

NIST: NIST SP 800-53A (v1): CM-3.1 (vii)

---

**CCI:** CCI-000320
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2009-09-17
**Definition:** The organization defines the frequency with which to convene the configuration change control element.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CM-3 f
NIST: NIST SP 800-53 Revision 4 (v4): CM-3 g
NIST: NIST SP 800-53A (v1): CM-3.1 (vi)

---

**CCI:** CCI-000321
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2009-09-17
**Definition:** The organization defines configuration change conditions that prompt the configuration change control element to convene.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CM-3 f
NIST: NIST SP 800-53 Revision 4 (v4): CM-3 g
NIST: NIST SP 800-53A (v1): CM-3.1 (vi)

---

**CCI:** CCI-000322
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2009-09-17
**Definition:** The organization employs automated mechanisms to document proposed changes to the information system.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CM-3 (1) (a)
NIST: NIST SP 800-53 Revision 4 (v4): CM-3 (1) (a)
NIST: NIST SP 800-53A (v1): CM-3 (1).1 (ii)

---

**CCI:** CCI-000323
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2009-09-17
**Definition:** The organization employs automated mechanisms to notify organization-defined approval authorities of proposed changes to the information system and request change approval.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CM-3 (1) (b)
NIST: NIST SP 800-53 Revision 4 (v4): CM-3 (1) (b)
NIST: NIST SP 800-53A (v1): CM-3 (1).1 (ii)

---

**CCI:** CCI-001742
**Status:** draft
**Contributor:** DISA FSO
**Published** 2013-02-28

**Date:**

**Definition:** The organization defines the approval authorities to be notified when proposed changes to the information system are received.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-3 (1) (b)

---

**CCI:** CCI-000324 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-17

**Definition:** The organization employs automated mechanisms to highlight proposed changes to the information system that have not been approved or disapproved by an organization-defined time period.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-3 (1) (c)
NIST: NIST SP 800-53 Revision 4 (v4): CM-3 (1) (c)
NIST: NIST SP 800-53A (v1): CM-3 (1).1 (ii)

---

**CCI:** CCI-001498 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-29

**Definition:** The organization defines a time period after which proposed changes to the information system that have not been approved or disapproved are highlighted.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-3 (1) (c)
NIST: NIST SP 800-53 Revision 4 (v4): CM-3 (1) (c)
NIST: NIST SP 800-53A (v1): CM-3 (1).1 (i)

---

**CCI:** CCI-000325 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-17

**Definition:** The organization employs automated mechanisms to prohibit changes to the information system until designated approvals are received.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-3 (1) (d)
NIST: NIST SP 800-53 Revision 4 (v4): CM-3 (1) (d)
NIST: NIST SP 800-53A (v1): CM-3 (1).1 (ii)

---

**CCI:** CCI-000326 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-17

**Definition:** The organization employs automated mechanisms to document all changes to the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-3 (1) (e)

NIST: NIST SP 800-53 Revision 4 (v4): CM-3 (1) (e)<br>
NIST: NIST SP 800-53A (v1): CM-3 (1).1 (ii)

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002057 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-11 |
| **Definition:** | The organization defines the personnel to be notified when approved changes to the information system are completed. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CM-3 (1) (f) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002058 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-11 |
| **Definition:** | The organization employs automated mechanisms to notify organization-defined personnel when approved changes to the information system are completed. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CM-3 (1) (f) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000327 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |
| **Definition:** | The organization tests changes to the information system before implementing the changes on the operational system. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CM-3 (2)<br>NIST: NIST SP 800-53 Revision 4 (v4): CM-3 (2)<br>NIST: NIST SP 800-53A (v1): CM-3 (2).1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000328 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |
| **Definition:** | The organization validates changes to the information system before implementing the changes on the operational system. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CM-3 (2)<br>NIST: NIST SP 800-53 Revision 4 (v4): CM-3 (2)<br>NIST: NIST SP 800-53A (v1): CM-3 (2).1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000329 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |
| **Definition:** | The organization documents changes to the information system before implementing the changes on the operational system. | | |

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-3 (2)
NIST: NIST SP 800-53 Revision 4 (v4): CM-3 (2)
NIST: NIST SP 800-53A (v1): CM-3 (2).1

---

**CCI:** CCI-000330 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-17

**Definition:** The organization employs automated mechanisms to implement changes to the current information system baseline.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-3 (3)
NIST: NIST SP 800-53 Revision 4 (v4): CM-3 (3)
NIST: NIST SP 800-53A (v1): CM-3 (3).1

---

**CCI:** CCI-000331 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-17

**Definition:** The organization deploys the updated information system baseline across the installed base.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-3 (3)
NIST: NIST SP 800-53 Revision 4 (v4): CM-3 (3)
NIST: NIST SP 800-53A (v1): CM-3 (3).1

---

**CCI:** CCI-000332 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-17

**Definition:** The organization requires an information security representative to be a member of the organization-defined configuration change control element.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-3 (4)
NIST: NIST SP 800-53 Revision 4 (v4): CM-3 (4)
NIST: NIST SP 800-53A (v1): CM-3 (3).1

---

**CCI:** CCI-001743 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-02-28

**Definition:** The organization defines the security responses to be automatically implemented by the information system if baseline configurations are changed in an unauthorized manner.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-3 (5)

---

**CCI:** CCI-001744 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-02-28

**Definition:** The information system implements organization-defined security responses automatically if baseline configurations are changed in an unauthorized manner.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-3 (5)

---

**CCI:** CCI-001745 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-02-28

**Definition:** The organization defines the security safeguards that are to be provided by the cryptographic mechanisms which are employed by the organization.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-3 (6)

---

**CCI:** CCI-001746 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-02-28

**Definition:** The organization ensures that cryptographic mechanisms used to provide organization-defined security safeguards are under configuration management.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-3 (6)

---

**CCI:** CCI-000333 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-4
NIST: NIST SP 800-53 Revision 4 (v4): CM-4
NIST: NIST SP 800-53A (v1): CM-4.1

---

**CCI:** CCI-001817 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-03-01

**Definition:** The organization, when analyzing changes to the information system, looks for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-4 (1)

---

**CCI:** CCI-001818 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-03-01

**Definition:** The organization analyzes changes to the information system in a separate test environment before installation in an operational environment.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-4 (1)

---

**CCI:** CCI-000335 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization, after the information system is changed, checks the security functions to verify the functions are implemented correctly.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-4 (2)
NIST: NIST SP 800-53 Revision 4 (v4): CM-4 (2)
NIST: NIST SP 800-53A (v1): CM-4 (2).1

---

**CCI:** CCI-000336 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization, after the information system is changed, checks the security functions to verify the functions are operating as intended.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-4 (2)
NIST: NIST SP 800-53 Revision 4 (v4): CM-4 (2)
NIST: NIST SP 800-53A (v1): CM-4 (2).1

---

**CCI:** CCI-000337 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization, after the information system is changed, checks the security functions to verify the functions are producing the desired outcome with regard to meeting the security requirements for the system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-4 (2)
NIST: NIST SP 800-53 Revision 4 (v4): CM-4 (2)
NIST: NIST SP 800-53A (v1): CM-4 (2).1

---

**CCI:** CCI-000338 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization defines physical access restrictions associated with changes to the information system.

**Type:** policy

**Note:** Defined by Homeland Security Presidential Directive 12 (HSPD 12)

**References:** NIST: NIST SP 800-53 (v3): CM-5
NIST: NIST SP 800-53 Revision 4 (v4): CM-5

NIST: NIST SP 800-53A (v1): CM-5.1

---

**CCI:** CCI-000339 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization documents physical access restrictions associated with changes to the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-5

NIST: NIST SP 800-53 Revision 4 (v4): CM-5

NIST: NIST SP 800-53A (v1): CM-5.1

---

**CCI:** CCI-000340 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization approves physical access restrictions associated with changes to the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-5

NIST: NIST SP 800-53 Revision 4 (v4): CM-5

NIST: NIST SP 800-53A (v1): CM-5.1

---

**CCI:** CCI-000341 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization enforces physical access restrictions associated with changes to the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-5

NIST: NIST SP 800-53 Revision 4 (v4): CM-5

NIST: NIST SP 800-53A (v1): CM-5.1

---

**CCI:** CCI-000342 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization defines logical access restrictions associated with changes to the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-5

NIST: NIST SP 800-53 Revision 4 (v4): CM-5

NIST: NIST SP 800-53A (v1): CM-5.1

---

**CCI:** CCI-000343 **Status:** draft

**Contributor:** DISA FSO **Published** 2009-09-18

| | | | |
|---|---|---|---|
| | | **Date:** | |
| **Definition:** | The organization documents logical access restrictions associated with changes to the information system. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CM-5<br>NIST: NIST SP 800-53 Revision 4 (v4): CM-5<br>NIST: NIST SP 800-53A (v1): CM-5.1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000344 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |
| **Definition:** | The organization approves logical access restrictions associated with changes to the information system. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CM-5<br>NIST: NIST SP 800-53 Revision 4 (v4): CM-5<br>NIST: NIST SP 800-53A (v1): CM-5.1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000345 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |
| **Definition:** | The organization enforces logical access restrictions associated with changes to the information system. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CM-5<br>NIST: NIST SP 800-53 Revision 4 (v4): CM-5<br>NIST: NIST SP 800-53A (v1): CM-5.1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001813 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-03-01 |
| **Definition:** | The information system enforces access restrictions. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CM-5 (1) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001814 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-03-01 |
| **Definition:** | The Information system supports auditing of the enforcement actions. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CM-5 (1) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000348 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published** | 2009-09-18 |

**Date:**

**Definition:** The organization defines a frequency with which to conduct reviews of information system changes.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-5 (2)
NIST: NIST SP 800-53 Revision 4 (v4): CM-5 (2)
NIST: NIST SP 800-53A (v1): CM-5 (2).1 (i)

---

**CCI:** CCI-000349 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization reviews information system changes per organization-defined frequency to determine whether unauthorized changes have occurred.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-5 (2)
NIST: NIST SP 800-53 Revision 4 (v4): CM-5 (2)
NIST: NIST SP 800-53A (v1): CM-5 (2).1 (ii)

---

**CCI:** CCI-000350 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization reviews information system changes upon organization-defined circumstances to determine whether unauthorized changes have occurred.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-5 (2)
NIST: NIST SP 800-53 Revision 4 (v4): CM-5 (2)
NIST: NIST SP 800-53A (v1): CM-5 (2).1 (ii)

---

**CCI:** CCI-001826 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-03-05

**Definition:** The organization defines the circumstances upon which the organization reviews the information system changes to determine whether unauthorized changes have occurred.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-5 (2)

---

**CCI:** CCI-001747 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-02-28

**Definition:** The organization defines critical software components the information system will prevent from being installed without verification the component has been digitally signed using a certificate that is recognized and approved by the organization.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-5 (3)

---

**CCI:** CCI-001748
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2013-02-28
**Definition:** The organization defines critical firmware components the information system will prevent from being installed without verification the component has been digitally signed using a certificate that is recognized and approved by the organization.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-5 (3)

---

**CCI:** CCI-001749
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2013-02-28
**Definition:** The information system prevents the installation of organization-defined software components without verification the software component has been digitally signed using a certificate that is recognized and approved by the organization.
**Type:** technical
**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-5 (3)

---

**CCI:** CCI-001750
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2013-02-28
**Definition:** The information system prevents the installation of organization-defined firmware components without verification the firmware component has been digitally signed using a certificate that is recognized and approved by the organization.
**Type:** technical
**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-5 (3)

---

**CCI:** CCI-000353
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2009-09-18
**Definition:** The organization defines information system components requiring enforcement of a dual authorization for information system changes.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CM-5 (4)
NIST: NIST SP 800-53 Revision 4 (v4): CM-5 (4)
NIST: NIST SP 800-53A (v1): CM-5 (4).1 (i)

---

**CCI:** CCI-000354
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2009-09-18
**Definition:** The organization enforces dual authorization for changes to organization-defined information system components.
**Type:** policy, technical
**References:** NIST: NIST SP 800-53 (v3): CM-5 (4)
NIST: NIST SP 800-53 Revision 4 (v4): CM-5 (4)

| | | | |
|---|---|---|---|
| | NIST: NIST SP 800-53A (v1): CM-5 (4).1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001751 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-02-28 |
| **Definition:** | The organization defines system-level information requiring enforcement of a dual authorization for information system changes. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CM-5 (4) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001752 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-02-28 |
| **Definition:** | The organization enforces dual authorization for changes to organization-defined system-level information. | | |
| **Type:** | policy, technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CM-5 (4) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001753 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-02-28 |
| **Definition:** | The organization limits privileges to change information system components within a production or operational environment. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CM-5 (5) (a) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001754 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-02-28 |
| **Definition:** | The organization limits privileges to change system-related information within a production or operational environment. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CM-5 (5) (a) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001827 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-03-05 |
| **Definition:** | The organization defines the frequency with which to review information system privileges. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CM-5 (5) (b) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001828 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-03-05 |

**Definition:** The organization defines the frequency with which to reevaluate information system privileges.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-5 (5) (b)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001829 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-03-05 |

**Definition:** The organization reviews information system privileges per an organization-defined frequency.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-5 (5) (b)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001830 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-03-05 |

**Definition:** The organization reevaluates information system privileges per an organization-defined frequency.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-5 (5) (b)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001499 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-29 |

**Definition:** The organization limits privileges to change software resident within software libraries.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): CM-5 (6)
NIST: NIST SP 800-53 Revision 4 (v4): CM-5 (6)
NIST: NIST SP 800-53A (v1): CM-5 (6).1

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001588 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-12 |

**Definition:** The organization-defined security configuration checklists reflect the most restrictive mode consistent with operational requirements.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-6 a
NIST: NIST SP 800-53 Revision 4 (v4): CM-6 a
NIST: NIST SP 800-53A (v1): CM-6.1 (ii)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000363 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |

**Definition:** The organization defines security configuration checklists to be used to establish and document configuration settings for the information system technology products employed.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-6 a
NIST: NIST SP 800-53 Revision 4 (v4): CM-6 a
NIST: NIST SP 800-53A (v1): CM-6.1 (i)

---

**CCI:** CCI-000364 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization establishes configuration settings for information technology products employed within the information system using organization-defined security configuration checklists.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-6 a
NIST: NIST SP 800-53 Revision 4 (v4): CM-6 a
NIST: NIST SP 800-53A (v1): CM-6.1 (iii)

---

**CCI:** CCI-000365 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization documents configuration settings for information technology products employed within the information system using organization-defined security configuration checklists that reflect the most restrictive mode consistent with operational requirements.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-6 a
NIST: NIST SP 800-53 Revision 4 (v4): CM-6 a
NIST: NIST SP 800-53A (v1): CM-6.1 (iii)

---

**CCI:** CCI-000366 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization implements the security configuration settings.

**Type:** policy, technical

**References:** NIST: NIST SP 800-53 (v3): CM-6 b
NIST: NIST SP 800-53 Revision 4 (v4): CM-6 b
NIST: NIST SP 800-53A (v1): CM-6.1 (iv)

---

**CCI:** CCI-000367 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization identifies any deviations from the established configuration settings for organization-defined information system components based on organization-defined operational requirements.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-6 c
NIST: NIST SP 800-53 Revision 4 (v4): CM-6 c
NIST: NIST SP 800-53A (v1): CM-6.1 (v)

---

**CCI:** CCI-000368 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-18
**Definition:** The organization documents any deviations from the established configuration settings for organization-defined information system components based on organization-defined operational requirements.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CM-6 c
NIST: NIST SP 800-53 Revision 4 (v4): CM-6 c
NIST: NIST SP 800-53A (v1): CM-6.1 (v)

---

**CCI:** CCI-000369 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-18
**Definition:** The organization approves any deviations from the established configuration settings for organization-defined information system components based on organization-defined operational requirements.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CM-6 c
NIST: NIST SP 800-53 Revision 4 (v4): CM-6 c
NIST: NIST SP 800-53A (v1): CM-6.1 (v)

---

**CCI:** CCI-001755 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-02-28
**Definition:** The organization defines the information system components for which any deviation from the established configuration settings are to be identified, documented, and approved.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-6 c

---

**CCI:** CCI-001756 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-02-28
**Definition:** The organization defines the operational requirements on which the configuration settings for the organization-defined information system components are to be based.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-6 c

---

**CCI:** CCI-001502 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-29

**Definition:** The organization monitors changes to the configuration settings in accordance with organizational policies and procedures.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-6 d
NIST: NIST SP 800-53 Revision 4 (v4): CM-6 d
NIST: NIST SP 800-53A (v1): CM-6.1 (vi)

---

**CCI:** CCI-001503 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-29

**Definition:** The organization controls changes to the configuration settings in accordance with organizational policies and procedures.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-6 d
NIST: NIST SP 800-53 Revision 4 (v4): CM-6 d
NIST: NIST SP 800-53A (v1): CM-6.1 (vi)

---

**CCI:** CCI-000370 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization employs automated mechanisms to centrally manage configuration settings for organization-defined information system components.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-6 (1)
NIST: NIST SP 800-53 Revision 4 (v4): CM-6 (1)
NIST: NIST SP 800-53A (v1): CM-6 (1).1

---

**CCI:** CCI-000371 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization employs automated mechanisms to centrally apply configuration settings for organization-defined information system components.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-6 (1)
NIST: NIST SP 800-53 Revision 4 (v4): CM-6 (1)
NIST: NIST SP 800-53A (v1): CM-6 (1).1

---

**CCI:** CCI-000372 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization employs automated mechanisms to centrally verify configuration settings for organization-defined information system components.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-6 (1)

NIST: NIST SP 800-53 Revision 4 (v4): CM-6 (1)
NIST: NIST SP 800-53A (v1): CM-6 (1).1

---

**CCI:** CCI-002059 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-06-11
**Definition:** The organization defines the information system components for which the organization will employ automated mechanisms to centrally manage, apply, and verify configuration settings.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-6 (1)

---

**CCI:** CCI-001757 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-02-28
**Definition:** The organization defines the security safeguards the organization is to employ when responding to unauthorized changes to the organization-defined configuration settings.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-6 (2)

---

**CCI:** CCI-001758 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-02-28
**Definition:** The organization defines configuration settings for which the organization will employ organization-defined security safeguards in response to unauthorized changes.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-6 (2)

---

**CCI:** CCI-001759 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-02-28
**Definition:** The organization employs organization-defined security safeguards to respond to unauthorized changes to organization-defined configuration settings.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-6 (2)

---

**CCI:** CCI-000381 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-18
**Definition:** The organization configures the information system to provide only essential capabilities.
**Type:** technical
**References:** NIST: NIST SP 800-53 (v3): CM-7
NIST: NIST SP 800-53 Revision 4 (v4): CM-7 a
NIST: NIST SP 800-53A (v1): CM-7.1 (ii)

---

**CCI:** CCI-000380 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-18
**Definition:** The organization defines prohibited or restricted functions, ports, protocols, and/or services for the information system.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CM-7
NIST: NIST SP 800-53 Revision 4 (v4): CM-7 b
NIST: NIST SP 800-53A (v1): CM-7.1 (i)

---

**CCI:** CCI-000382 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-18
**Definition:** The organization configures the information system to prohibit or restrict the use of organization-defined functions, ports, protocols, and/or services.
**Type:** technical
**References:** NIST: NIST SP 800-53 (v3): CM-7
NIST: NIST SP 800-53 Revision 4 (v4): CM-7 b
NIST: NIST SP 800-53A (v1): CM-7.1 (iii)

---

**CCI:** CCI-000384 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-18
**Definition:** The organization reviews the information system per organization-defined frequency to identify unnecessary and nonsecure functions, ports, protocols, and services.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CM-7 (1)
NIST: NIST SP 800-53 Revision 4 (v4): CM-7 (1) (a)
NIST: NIST SP 800-53A (v1): CM-7 (1).1 (i)

---

**CCI:** CCI-001760 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-02-28
**Definition:** The organization defines the frequency of information system reviews to identify unnecessary and/or nonsecure functions, ports, protocols, and services.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-7 (1) (a)

---

**CCI:** CCI-001761 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-02-28
**Definition:** The organization defines the functions, ports, protocols, and services within the information system that are to be disabled when deemed unnecessary and/or nonsecure.
**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-7 (1) (b)

---

**CCI:** CCI-001762 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-02-28

**Definition:** The organization disables organization-defined functions, ports, protocols, and services within the information system deemed to be unnecessary and/or nonsecure.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-7 (1) (b)

---

**CCI:** CCI-001592 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2010-05-12

**Definition:** The organization defines the rules authorizing the terms and conditions of software program usage on the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-7 (2)
NIST: NIST SP 800-53 Revision 4 (v4): CM-7 (2)
NIST: NIST SP 800-53A (v1): CM-7 (2).1 (i)

---

**CCI:** CCI-001763 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-02-28

**Definition:** The organization defines the policies regarding software program usage and restrictions.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-7 (2)

---

**CCI:** CCI-001764 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-02-28

**Definition:** The information system prevents program execution in accordance with organization-defined policies regarding software program usage and restrictions, and/or rules authorizing the terms and conditions of software program usage.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-7 (2)

---

**CCI:** CCI-000387 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization defines registration requirements for functions, ports, protocols, and services.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-7 (3)
NIST: NIST SP 800-53 Revision 4 (v4): CM-7 (3)

| | | | |
|---|---|---|---|
| | NIST: NIST SP 800-53A (v1): CM- 7(3).1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000388 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |
| **Definition:** | The organization ensures compliance with organization-defined registration requirements for functions, ports, protocols, and services. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CM-7 (3)<br>NIST: NIST SP 800-53 Revision 4 (v4): CM-7 (3)<br>NIST: NIST SP 800-53A (v1): CM-7 (3).1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001765 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-02-28 |
| **Definition:** | The organization defines the software programs not authorized to execute on the information system. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CM-7 (4) (a) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001766 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-02-28 |
| **Definition:** | The organization identifies the organization-defined software programs not authorized to execute on the information system. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CM-7 (4) (a) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001767 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-02-28 |
| **Definition:** | The organization employs an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CM-7 (4) (b) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001768 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-02-28 |
| **Definition:** | The organization defines the frequency on which it will review and update the list of unauthorized software programs. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CM-7 (4) (c) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001769 | **Status:** | deprecated |

**Contributor:** DISA FSO **Published Date:** 2013-02-28

**Definition:** The organization defines the frequency on which it will update the list of unauthorized software programs.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-7 (4) (c)

---

**CCI:** CCI-001770 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-02-28

**Definition:** The organization reviews and updates the list of unauthorized software programs per organization-defined frequency.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-7 (4) (c)

---

**CCI:** CCI-001771 **Status:** deprecated

**Contributor:** DISA FSO **Published Date:** 2013-02-28

**Definition:** The organization updates the list of unauthorized software programs per organization-defined frequency.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-7 (4) (c)

---

**CCI:** CCI-001772 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-02-28

**Definition:** The organization defines the software programs authorized to execute on the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-7 (5) (a)

---

**CCI:** CCI-001773 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-02-28

**Definition:** The organization identifies the organization-defined software programs authorized to execute on the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-7 (5) (a)

---

**CCI:** CCI-001774 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-02-28

**Definition:** The organization employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-7 (5) (b)

---

**CCI:** CCI-001775 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-02-28

**Definition:** The organization defines the frequency on which it will review and update the list of authorized software programs.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-7 (5) (c)

---

**CCI:** CCI-001776 **Status:** deprecated

**Contributor:** DISA FSO **Published Date:** 2013-02-28

**Definition:** The organization defines the frequency on which it will update the list of authorized software programs.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-7 (5) (c)

---

**CCI:** CCI-001777 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-02-28

**Definition:** The organization reviews and updates the list of authorized software programs per organization-defined frequency.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-7 (5) (c)

---

**CCI:** CCI-001778 **Status:** deprecated

**Contributor:** DISA FSO **Published Date:** 2013-02-28

**Definition:** The organization updates the list of authorized software programs per organization-defined frequency.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-7 (5) (c)

---

**CCI:** CCI-000389 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization develops an inventory of information system components that accurately reflects the current information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-8 a

NIST: NIST SP 800-53 Revision 4 (v4): CM-8 a 1

NIST: NIST SP 800-53A (v1): CM-8.1 (ii)

---

**CCI:** CCI-000390 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization documents an inventory of information system components that accurately reflects the current information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-8 a

NIST: NIST SP 800-53 Revision 4 (v4): CM-8 a 1

NIST: NIST SP 800-53A (v1): CM-8.1 (ii)

---

**CCI:** CCI-000392 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization develops an inventory of information system components that includes all components within the authorization boundary of the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-8 b

NIST: NIST SP 800-53 Revision 4 (v4): CM-8 a 2

NIST: NIST SP 800-53A (v1): CM-8.1 (ii)

---

**CCI:** CCI-000393 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization documents an inventory of information system components that includes all components within the authorization boundary of the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-8 b

NIST: NIST SP 800-53 Revision 4 (v4): CM-8 a 2

NIST: NIST SP 800-53A (v1): CM-8.1 (ii)

---

**CCI:** CCI-000395 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization develops an inventory of information system components that is at the level of granularity deemed necessary for tracking and reporting.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-8 c

NIST: NIST SP 800-53 Revision 4 (v4): CM-8 a 3

NIST: NIST SP 800-53A (v1): CM-8.1 (ii)

---

**CCI:** CCI-000396 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization documents an inventory of information system components that is at the level of granularity deemed necessary for tracking and reporting.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-8 c
NIST: NIST SP 800-53 Revision 4 (v4): CM-8 a 3
NIST: NIST SP 800-53A (v1): CM-8.1 (ii)

---

**CCI:** CCI-000398 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization defines information deemed necessary to achieve effective information system component accountability.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-8 d
NIST: NIST SP 800-53 Revision 4 (v4): CM-8 a 4
NIST: NIST SP 800-53A (v1): CM-8.1 (i)

---

**CCI:** CCI-000399 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization develops an inventory of information system components that includes organization-defined information deemed necessary to achieve effective information system component accountability.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-8 d
NIST: NIST SP 800-53 Revision 4 (v4): CM-8 a 4
NIST: NIST SP 800-53A (v1): CM-8.1 (ii)

---

**CCI:** CCI-000400 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization documents an inventory of information system components that includes organization-defined information deemed necessary to achieve effective information system component accountability.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-8 d
NIST: NIST SP 800-53 Revision 4 (v4): CM-8 a 4
NIST: NIST SP 800-53A (v1): CM-8.1 (ii)

---

**CCI:** CCI-001779 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-02-28

**Definition:** The organization defines the frequency on which the information system component inventory is to be reviewed and updated.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-8 b

---

**CCI:** CCI-001780
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2013-02-28
**Definition:** The organization reviews and updates the information system component inventory per organization-defined frequency.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-8 b

---

**CCI:** CCI-001781
**Status:** deprecated
**Contributor:** DISA FSO
**Published Date:** 2013-03-01
**Definition:** The organization defines the frequency on which the information system component inventory is to be updated.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-8 b

---

**CCI:** CCI-001782
**Status:** deprecated
**Contributor:** DISA FSO
**Published Date:** 2013-03-01
**Definition:** The organization updates the information system component inventory per organization-defined frequency.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-8 b

---

**CCI:** CCI-000408
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2009-09-18
**Definition:** The organization updates the inventory of information system components as an integral part of component installations.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CM-8 (1)
NIST: NIST SP 800-53 Revision 4 (v4): CM-8 (1)
NIST: NIST SP 800-53A (v1): CM-8 (1).1

---

**CCI:** CCI-000409
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2009-09-18
**Definition:** The organization updates the inventory of information system components as an integral part of component removals.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CM-8 (1)
NIST: NIST SP 800-53 Revision 4 (v4): CM-8 (1)

NIST: NIST SP 800-53A (v1): CM-8 (1).1

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000410 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |
| **Definition:** | The organization updates the inventory of information system components as an integral part of information system updates. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CM-8 (1)<br>NIST: NIST SP 800-53 Revision 4 (v4): CM-8 (1)<br>NIST: NIST SP 800-53A (v1): CM-8 (1).1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000411 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |
| **Definition:** | The organization employs automated mechanisms to help maintain an up-to-date inventory of information system components. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CM-8 (2)<br>NIST: NIST SP 800-53 Revision 4 (v4): CM-8 (2)<br>NIST: NIST SP 800-53A (v1): CM-8 (2).1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000412 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |
| **Definition:** | The organization employs automated mechanisms to help maintain a complete inventory of information system components. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CM-8 (2)<br>NIST: NIST SP 800-53 Revision 4 (v4): CM-8 (2)<br>NIST: NIST SP 800-53A (v1): CM-8 (2).1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000413 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |
| **Definition:** | The organization employs automated mechanisms to help maintain an accurate inventory of information system components. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CM-8 (2)<br>NIST: NIST SP 800-53 Revision 4 (v4): CM-8 (2)<br>NIST: NIST SP 800-53A (v1): CM-8 (2).1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000414 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published** | 2009-09-18 |

**Date:**

**Definition:** The organization employs automated mechanisms to help maintain a readily available inventory of information system components.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-8 (2)
NIST: NIST SP 800-53 Revision 4 (v4): CM-8 (2)
NIST: NIST SP 800-53A (v1): CM-8 (2).1

---

**CCI:** CCI-000415 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization defines the frequency of employing automated mechanisms to detect the presence of unauthorized hardware, software, and firmware components within the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-8 (3) (a)
NIST: NIST SP 800-53 Revision 4 (v4): CM-8 (3) (a)
NIST: NIST SP 800-53A (v1): CM-8 (3).1 (i)

---

**CCI:** CCI-000416 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization employs automated mechanisms, per organization-defined frequency, to detect the presence of unauthorized hardware, software, and firmware components within the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-8 (3) (a)
NIST: NIST SP 800-53 Revision 4 (v4): CM-8 (3) (a)
NIST: NIST SP 800-53A (v1): CM-8 (3).1 (ii)

---

**CCI:** CCI-001783 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-03-01

**Definition:** The organization defines the personnel or roles to be notified when unauthorized hardware, software, and firmware components are detected within the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-8 (3) (b)

---

**CCI:** CCI-001784 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-03-01

**Definition:** When unauthorized hardware, software, and firmware components are detected within the information system, the organization takes action to disable network access by such components, isolates the components, and/or notifies organization-defined personnel or roles.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-8 (3) (b)

---

**CCI:** CCI-000418  
**Status:** draft

**Contributor:** DISA FSO  
**Published Date:** 2009-09-18

**Definition:** The organization includes, in the information system component inventory information, a means for identifying by name, position, and/or role, individuals responsible/accountable for administering those components.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-8 (4)  
NIST: NIST SP 800-53 Revision 4 (v4): CM-8 (4)  
NIST: NIST SP 800-53A (v1): CM-8 (4).1

---

**CCI:** CCI-000419  
**Status:** draft

**Contributor:** DISA FSO  
**Published Date:** 2009-09-18

**Definition:** The organization verifies that all components within the authorization boundary of the information system are not duplicated in other information system component inventories.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-8 (5)  
NIST: NIST SP 800-53 Revision 4 (v4): CM-8 (5)  
NIST: NIST SP 800-53A (v1): CM-8 (5).1

---

**CCI:** CCI-000420  
**Status:** draft

**Contributor:** DISA FSO  
**Published Date:** 2009-09-18

**Definition:** The organization includes assessed component configurations and any approved deviations to current deployed configurations in the information system component inventory.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-8 (6)  
NIST: NIST SP 800-53 Revision 4 (v4): CM-8 (6)  
NIST: NIST SP 800-53A (v1): CM-8 (6).1

---

**CCI:** CCI-001785  
**Status:** draft

**Contributor:** DISA FSO  
**Published Date:** 2013-03-01

**Definition:** The organization provides a centralized repository for the inventory of information system components.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-8 (7)

---

**CCI:** CCI-001786  
**Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-03-01

**Definition:** The organization employs automated mechanisms to support tracking of information system components by geographic location.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-8 (8)

---

**CCI:** CCI-001787 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-03-01

**Definition:** The organization defines the acquired information system components that are to be assigned to an information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-8 (9) (a)

---

**CCI:** CCI-001788 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-03-01

**Definition:** The organization assigns organization-defined acquired information system components to an information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-8 (9) (a)

---

**CCI:** CCI-001789 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-03-01

**Definition:** The organization receives an acknowledgement from the information system owner of the assignment of the acquired information system components to an information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-8 (9) (b)

---

**CCI:** CCI-000421 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization develops a configuration management plan for the information system that addresses roles, responsibilities, and configuration management processes and procedures.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-9 a
NIST: NIST SP 800-53 Revision 4 (v4): CM-9 a
NIST: NIST SP 800-53A (v1): CM-9.1 (i)

---

**CCI:** CCI-000422 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization documents a configuration management plan for the information system that addresses roles, responsibilities, and configuration management processes and procedures.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-9 a
NIST: NIST SP 800-53 Revision 4 (v4): CM-9 a
NIST: NIST SP 800-53A (v1): CM-9.1 (i)

---

**CCI:** CCI-000423 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization implements a configuration management plan for the information system that addresses roles, responsibilities, and configuration management processes and procedures.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-9 a
NIST: NIST SP 800-53 Revision 4 (v4): CM-9 a
NIST: NIST SP 800-53A (v1): CM-9.1 (i)

---

**CCI:** CCI-001790 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-03-01

**Definition:** The organization develops a configuration management plan for the information system that establishes a process for identifying configuration items throughout the system development life cycle.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-9 b

---

**CCI:** CCI-001791 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-03-01

**Definition:** The organization documents a configuration management plan for the information system that establishes a process for identifying configuration items throughout the system development life cycle.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-9 b

---

**CCI:** CCI-001792 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-03-01

**Definition:** The organization implements a configuration management plan for the information system that establishes a process for identifying configuration items throughout the system development life cycle.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-9 b

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001793 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-03-01 |
| **Definition:** | The organization develops a configuration management plan for the information system that establishes a process for managing the configuration of the configuration items. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CM-9 b | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001794 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-03-01 |
| **Definition:** | The organization documents a configuration management plan for the information system that establishes a process for managing the configuration of the configuration items. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CM-9 b | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001795 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-03-01 |
| **Definition:** | The organization implements a configuration management plan for the information system that establishes a process for managing the configuration of the configuration items. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CM-9 b | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000424 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |
| **Definition:** | The organization develops a configuration management plan for the information system that defines the configuration items for the information system. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CM-9 b<br>NIST: NIST SP 800-53 Revision 4 (v4): CM-9 c<br>NIST: NIST SP 800-53A (v1): CM-9.1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000425 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |
| **Definition:** | The organization documents a configuration management plan for the information system that defines the configuration items for the information system. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CM-9 b<br>NIST: NIST SP 800-53 Revision 4 (v4): CM-9 c<br>NIST: NIST SP 800-53A (v1): CM-9.1 (i) | | |

**CCI:** CCI-000426
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2009-09-18
**Definition:** The organization implements a configuration management plan for the information system that defines the configuration items for the information system.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CM-9 b
NIST: NIST SP 800-53 Revision 4 (v4): CM-9 c
NIST: NIST SP 800-53A (v1): CM-9.1 (i)

---

**CCI:** CCI-001796
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2013-03-01
**Definition:** The organization develops a configuration management plan for the information system that places the configuration items under configuration management.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-9 c

---

**CCI:** CCI-001797
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2013-03-01
**Definition:** The organization documents a configuration management plan for the information system that places the configuration items under configuration management.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-9 c

---

**CCI:** CCI-001798
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2013-03-01
**Definition:** The organization implements a configuration management plan for the information system that places the configuration items under configuration management.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-9 c

---

**CCI:** CCI-001799
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2013-03-01
**Definition:** The organization develops and documents a configuration management plan for the information system that protects the configuration management plan from unauthorized disclosure and modification.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-9 d

---

**CCI:** CCI-001800
**Status:** deprecated
**Contributor:** DISA FSO
**Published** 2013-03-01

**Date:**

**Definition:** The organization documents a configuration management plan for the information system that protects the configuration management plan from unauthorized disclosure and modification.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-9 d

---

**CCI:** CCI-001801 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-03-01

**Definition:** The organization implements a configuration management plan for the information system that protects the configuration management plan from unauthorized disclosure and modification.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-9 d

---

**CCI:** CCI-000436 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization assigns responsibility for developing the configuration management process to organizational personnel that are not directly involved in information system development.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-9 (1)
NIST: NIST SP 800-53 Revision 4 (v4): CM-9 (1)
NIST: NIST SP 800-53A (v1): CM-9 (1).1

---

**CCI:** CCI-001726 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-02-28

**Definition:** The organization uses software in accordance with contract agreements.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-10 a

---

**CCI:** CCI-001727 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-02-28

**Definition:** The organization uses software documentation in accordance with contract agreements.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-10 a

---

**CCI:** CCI-001728 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-02-28

**Definition:** The organization uses software in accordance with copyright laws.

| | | | |
|---|---|---|---|
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CM-10 a | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001729 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-02-28 |
| **Definition:** | The organization uses software documentation in accordance with copyright laws. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CM-10 a | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001730 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-02-28 |
| **Definition:** | The organization tracks the use of software protected by quantity licenses to control copying of the software. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CM-10 b | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001731 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-02-28 |
| **Definition:** | The organization tracks the use of software documentation protected by quantity licenses to control distribution of the software documentation. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CM-10 b | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001802 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-03-01 |
| **Definition:** | The organization tracks the use of software documentation protected by quantity licenses to control copying of the software documentation. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CM-10 b | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001803 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-03-01 |
| **Definition:** | The organization tracks the use of software protected by quantity licenses to control distribution of the software. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CM-10 b | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001732 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published** | 2013-02-28 |

**Date:**

**Definition:** The organization controls the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-10 c

---

**CCI:** CCI-001733 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-02-28

**Definition:** The organization documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-10 c

---

**CCI:** CCI-001734 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-02-28

**Definition:** The organization defines the restrictions to be followed on the use of open source software.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-10 (1)

---

**CCI:** CCI-001735 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-02-28

**Definition:** The organization establishes organization-defined restrictions on the use of open source software.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-10 (1)

---

**CCI:** CCI-001804 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-03-01

**Definition:** The organization defines the policies for governing the installation of software by users.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-11 a

---

**CCI:** CCI-001805 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-03-01

**Definition:** The organization establishes organization-defined policies governing the installation of software by users.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CM-11 a

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001806 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-03-01 |
| **Definition:** | The organization defines methods to be employed to enforce the software installation policies. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CM-11 b | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001807 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-03-01 |
| **Definition:** | The organization enforces software installation policies through organization-defined methods. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CM-11 b | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001808 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-03-01 |
| **Definition:** | The organization defines the frequency on which it will monitor software installation policy compliance. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CM-11 c | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001809 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-03-01 |
| **Definition:** | The organization monitors software installation policy compliance per an organization-defined frequency. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CM-11 c | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001810 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-03-01 |
| **Definition:** | The organization defines the personnel or roles to be notified when unauthorized software is detected. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CM-11 (1) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001811 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-03-01 |
| **Definition:** | The information system alerts organization-defined personnel or roles when the | | |

| | | | |
|---|---|---|---|
| | unauthorized installation of software is detected. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CM-11 (1) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001812 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-03-01 |
| **Definition:** | The information system prohibits user installation of software without explicit privileged status. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CM-11 (2) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001597 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-12 |
| **Definition:** | The organization disseminates contingency planning procedures to organization-defined personnel or roles. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CP-1<br>NIST: NIST SP 800-53 Revision 4 (v4): CP-1 a 2<br>NIST: NIST SP 800-53A (v1): CP-1.1 (vi) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000438 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |
| **Definition:** | The organization develops and documents a contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CP-1 a<br>NIST: NIST SP 800-53 Revision 4 (v4): CP-1 a 1<br>NIST: NIST SP 800-53A (v1): CP-1.1 (i) (ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000439 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |
| **Definition:** | The organization disseminates a contingency planning policy to organization-defined personnel or roles. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CP-1 a<br>NIST: NIST SP 800-53 Revision 4 (v4): CP-1 a 1<br>NIST: NIST SP 800-53A (v1): CP-1.1 (iii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000441 | **Status:** | draft |

| | | | |
|---|---|---|---|
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |

**Definition:** The organization develops and documents procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-1 b
NIST: NIST SP 800-53 Revision 4 (v4): CP-1 a 2
NIST: NIST SP 800-53A (v1): CP-1.1 (iv) (v)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002825 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-20 |

**Definition:** The organization defines personnel or roles to whom the contingency planning policy is to be disseminated.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CP-1 a 1

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002826 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-20 |

**Definition:** The organization defines personnel or roles to whom the contingency planning procedures are disseminated.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CP-1 a 2

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001596 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-12 |

**Definition:** The organization defines the frequency with which to review and update the current contingency planning procedures.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-1
NIST: NIST SP 800-53 Revision 4 (v4): CP-1 b 2
NIST: NIST SP 800-53A (v1): CP-1.2 (iii)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001598 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-12 |

**Definition:** The organization reviews and updates the current contingency planning procedures in accordance with the organization-defined frequency.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-1
NIST: NIST SP 800-53 Revision 4 (v4): CP-1 b 2
NIST: NIST SP 800-53A (v1): CP-1.2 (iv)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000437 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |
| **Definition:** | The organization defines the frequency with which to review and update the current contingency planning policy. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CP-1<br>NIST: NIST SP 800-53 Revision 4 (v4): CP-1 b 1<br>NIST: NIST SP 800-53A (v1): CP-1.2 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000440 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |
| **Definition:** | The organization reviews and updates the current contingency planning policy in accordance with an organization-defined frequency. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CP-1 a<br>NIST: NIST SP 800-53 Revision 4 (v4): CP-1 b 1<br>NIST: NIST SP 800-53A (v1): CP-1.2 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000443 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |
| **Definition:** | The organization develops a contingency plan for the information system that identifies essential missions. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CP-2 a<br>NIST: NIST SP 800-53 Revision 4 (v4): CP-2 a 1<br>NIST: NIST SP 800-53A (v1): CP-2.1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000444 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |
| **Definition:** | The organization develops a contingency plan for the information system that identifies essential business functions. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CP-2 a<br>NIST: NIST SP 800-53 Revision 4 (v4): CP-2 a 1<br>NIST: NIST SP 800-53A (v1): CP-2.1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000445 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |
| **Definition:** | The organization develops a contingency plan for the information system that identifies | | |

associated contingency requirements.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-2 a
NIST: NIST SP 800-53 Revision 4 (v4): CP-2 a 1
NIST: NIST SP 800-53A (v1): CP-2.1 (i)

---

**CCI:** CCI-000446 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization develops a contingency plan for the information system that provides recovery objectives.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-2 a
NIST: NIST SP 800-53 Revision 4 (v4): CP-2 a 2
NIST: NIST SP 800-53A (v1): CP-2.1 (i)

---

**CCI:** CCI-000447 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization develops a contingency plan for the information system that provides restoration priorities.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-2 a
NIST: NIST SP 800-53 Revision 4 (v4): CP-2 a 2
NIST: NIST SP 800-53A (v1): CP-2.1 (i)

---

**CCI:** CCI-000448 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization develops a contingency plan for the information system that provides metrics.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-2 a
NIST: NIST SP 800-53 Revision 4 (v4): CP-2 a 2
NIST: NIST SP 800-53A (v1): CP-2.1 (i)

---

**CCI:** CCI-000449 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization develops a contingency plan for the information system that addresses contingency roles, responsibilities, assigned individuals with contact information.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-2 a
NIST: NIST SP 800-53 Revision 4 (v4): CP-2 a 3

NIST: NIST SP 800-53A (v1): CP-2.1 (i)

---

**CCI:** CCI-000450 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization develops a contingency plan for the information system that addresses maintaining essential missions despite an information system disruption.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-2 a

NIST: NIST SP 800-53 Revision 4 (v4): CP-2 a 4

NIST: NIST SP 800-53A (v1): CP-2.1 (i)

---

**CCI:** CCI-000451 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization develops a contingency plan for the information system that addresses maintaining essential business functions despite an information system disruption.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-2 a

NIST: NIST SP 800-53 Revision 4 (v4): CP-2 a 4

NIST: NIST SP 800-53A (v1): CP-2.1 l)

---

**CCI:** CCI-000452 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization develops a contingency plan for the information system that addresses maintaining essential missions despite an information system compromise.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-2 a

NIST: NIST SP 800-53 Revision 4 (v4): CP-2 a 4

NIST: NIST SP 800-53A (v1): CP-2.1 (i)

---

**CCI:** CCI-000453 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization develops a contingency plan for the information system that addresses maintaining essential business functions despite an information system compromise.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-2 a

NIST: NIST SP 800-53 Revision 4 (v4): CP-2 a 4

NIST: NIST SP 800-53A (v1): CP-2.1 (i)

---

**CCI:** CCI-000454 **Status:** draft

**Contributor:** DISA FSO **Published** 2009-09-18

**Date:**

**Definition:** The organization develops a contingency plan for the information system that addresses maintaining essential missions despite an information system failure.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-2 a  
NIST: NIST SP 800-53 Revision 4 (v4): CP-2 a 4  
NIST: NIST SP 800-53A (v1): CP-2.1 (i)

---

**CCI:** CCI-000455 **Status:** draft  
**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization develops a contingency plan for the information system that addresses maintaining essential business functions despite an information system failure.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-2 a  
NIST: NIST SP 800-53 Revision 4 (v4): CP-2 a 4  
NIST: NIST SP 800-53A (v1): CP-2.1 (i)

---

**CCI:** CCI-000456 **Status:** draft  
**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization develops a contingency plan for the information system that addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-2 a  
NIST: NIST SP 800-53 Revision 4 (v4): CP-2 a 5  
NIST: NIST SP 800-53A (v1): CP-2.1 (i)

---

**CCI:** CCI-000457 **Status:** draft  
**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization develops a contingency plan for the information system that is reviewed and approved by organization-defined personnel or roles.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-2 a  
NIST: NIST SP 800-53 Revision 4 (v4): CP-2 a 6  
NIST: NIST SP 800-53A (v1): CP-2.1 (i)

---

**CCI:** CCI-002830 **Status:** draft  
**Contributor:** DISA FSO **Published Date:** 2013-07-20

**Definition:** The organization defines the personnel or roles who review and approve the contingency plan for the information system.

| | |
|---|---|
| **Type:** | policy |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CP-2 a 6 |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000458 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |
| **Definition:** | The organization defines a list of key contingency personnel (identified by name and/or by role) and organizational elements designated to receive copies of the contingency plan. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CP-2 b<br>NIST: NIST SP 800-53 Revision 4 (v4): CP-2 b<br>NIST: NIST SP 800-53A (v1): CP-2.1 (ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000459 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |
| **Definition:** | The organization distributes copies of the contingency plan to an organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CP-2 b<br>NIST: NIST SP 800-53 Revision 4 (v4): CP-2 b<br>NIST: NIST SP 800-53A (v1): CP-2.1 (iii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000460 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |
| **Definition:** | The organization coordinates contingency planning activities with incident handling activities. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CP-2 c<br>NIST: NIST SP 800-53 Revision 4 (v4): CP-2 c<br>NIST: NIST SP 800-53A (v1): CP-2.2 (i) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000461 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |
| **Definition:** | The organization defines the frequency with which to review the contingency plan for the information system. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CP-2 c<br>NIST: NIST SP 800-53 Revision 4 (v4): CP-2 d<br>NIST: NIST SP 800-53A (v1): CP-2.2 (ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000462 | **Status:** | draft |

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization reviews the contingency plan for the information system in accordance with organization-defined frequency.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-2 c

NIST: NIST SP 800-53 Revision 4 (v4): CP-2 d

NIST: NIST SP 800-53A (v1): CP-2.2 (iii)

---

**CCI:** CCI-000463 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization updates the contingency plan to address changes to the organization.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-2 e

NIST: NIST SP 800-53 Revision 4 (v4): CP-2 e

NIST: NIST SP 800-53A (v1): CP-2.2 (iv)

---

**CCI:** CCI-000464 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization updates the contingency plan to address changes to the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-2 e

NIST: NIST SP 800-53 Revision 4 (v4): CP-2 e

NIST: NIST SP 800-53A (v1): CP-2.2 (iv)

---

**CCI:** CCI-000465 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization updates the contingency plan to address changes to the environment of operation.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-2 e

NIST: NIST SP 800-53 Revision 4 (v4): CP-2 e

NIST: NIST SP 800-53A (v1): CP-2.2 (iv)

---

**CCI:** CCI-000466 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization updates the contingency plan to address problems encountered during contingency plan implementation, execution, or testing.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-2 e
NIST: NIST SP 800-53 Revision 4 (v4): CP-2 e
NIST: NIST SP 800-53A (v1): CP-2.2 (iv)

---

**CCI:** CCI-000468 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-18
**Definition:** The organization communicates contingency plan changes to an organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements.
**Type:** policy
**Note:** This is nearly identical to CP-2 (e).
**References:** NIST: NIST SP 800-53 (v3): CP-2 f
NIST: NIST SP 800-53 Revision 4 (v4): CP-2 f
NIST: NIST SP 800-53A (v1): CP-2.2 (v)

---

**CCI:** CCI-002831 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-07-20
**Definition:** The organization defines a list of key contingency personnel (identified by name and/or by role) and organizational elements to whom contingency plan changes are to be communicated.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): CP-2 f

---

**CCI:** CCI-002832 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-07-20
**Definition:** The organization protects the contingency plan from unauthorized disclosure and modification.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): CP-2 g

---

**CCI:** CCI-000469 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-18
**Definition:** The organization coordinates contingency plan development with organizational elements responsible for related plans.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CP-2 (1)
NIST: NIST SP 800-53 Revision 4 (v4): CP-2 (1)
NIST: NIST SP 800-53A (v1): CP-2 (1).1

---

**CCI:** CCI-000470 **Status:** draft
**Contributor:** DISA FSO **Published** 2009-09-18

**Date:**

**Definition:** The organization conducts capacity planning so that necessary capacity for information processing exists during contingency operations.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-2 (2)
NIST: NIST SP 800-53 Revision 4 (v4): CP-2 (2)
NIST: NIST SP 800-53A (v1): CP-2 (2).1

---

**CCI:** CCI-000471 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization conducts capacity planning so that necessary capacity for telecommunications exists during contingency operations.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-2 (2)
NIST: NIST SP 800-53 Revision 4 (v4): CP-2 (2)
NIST: NIST SP 800-53A (v1): CP-2 (2).1

---

**CCI:** CCI-000472 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization conducts capacity planning so that necessary capacity for environmental support exists during contingency operations.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-2 (2)
NIST: NIST SP 800-53 Revision 4 (v4): CP-2 (2)
NIST: NIST SP 800-53A (v1): CP-2 (2).1

---

**CCI:** CCI-000473 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization defines the time period for planning the resumption of essential missions as a result of contingency plan activation.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-2 (3)
NIST: NIST SP 800-53 Revision 4 (v4): CP-2 (3)
NIST: NIST SP 800-53A (v1): CP-2 (3).1 (i)

---

**CCI:** CCI-000474 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization defines the time period for planning the resumption of essential business functions as a result of contingency plan activation.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-2 (3)
NIST: NIST SP 800-53 Revision 4 (v4): CP-2 (3)
NIST: NIST SP 800-53A (v1): CP-2 (3).1 (i)

---

**CCI:** CCI-000475 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-18
**Definition:** The organization plans for the resumption of essential missions within the organization-defined time period of contingency plan activation.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CP-2 (3)
NIST: NIST SP 800-53 Revision 4 (v4): CP-2 (3)
NIST: NIST SP 800-53A (v1): CP-2 (3).1 (ii)

---

**CCI:** CCI-000476 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-18
**Definition:** The organization plans for the resumption of essential business functions within the organization-defined time period of contingency plan activation.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CP-2 (3)
NIST: NIST SP 800-53 Revision 4 (v4): CP-2 (3)
NIST: NIST SP 800-53A (v1): CP-2 (3).1 (ii)

---

**CCI:** CCI-000477 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-18
**Definition:** The organization defines the time period for planning the resumption of all missions as a result of contingency plan activation.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CP-2 (4)
NIST: NIST SP 800-53 Revision 4 (v4): CP-2 (4)
NIST: NIST SP 800-53A (v1): CP-2 (4).1 (i)

---

**CCI:** CCI-000478 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-18
**Definition:** The organization defines the time period for planning the resumption of all business functions as a result of contingency plan activation.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CP-2 (4)
NIST: NIST SP 800-53 Revision 4 (v4): CP-2 (4)
NIST: NIST SP 800-53A (v1): CP-2 (4).1 (i)

---

**CCI:** CCI-000479 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization plans for the resumption of all missions within an organization-defined time period of contingency plan activation.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-2 (4)

NIST: NIST SP 800-53 Revision 4 (v4): CP-2 (4)

NIST: NIST SP 800-53A (v1): CP-2 (4).1 (ii)

---

**CCI:** CCI-000480 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization plans for the resumption of all business functions within an organization-defined time period of contingency plan activation.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-2 (4)

NIST: NIST SP 800-53 Revision 4 (v4): CP-2 (4)

NIST: NIST SP 800-53A (v1): CP-2 (4).1 (ii)

---

**CCI:** CCI-001599 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2010-05-12

**Definition:** The organization sustains operational continuity of essential missions until full information system restoration at primary processing and/or storage sites.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-2 (5)

NIST: NIST SP 800-53 Revision 4 (v4): CP-2 (5)

NIST: NIST SP 800-53A (v1): CP-2 (5).1 (b)

---

**CCI:** CCI-001600 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2010-05-12

**Definition:** The organization sustains operational continuity of essential business functions until full information system restoration at primary processing and/or storage sites.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-2 (5)

NIST: NIST SP 800-53 Revision 4 (v4): CP-2 (5)

NIST: NIST SP 800-53A (v1): CP-2 (5).1 (b)

---

**CCI:** CCI-000481 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization plans for the continuance of essential missions with little or no loss of operational continuity.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-2 (5)
NIST: NIST SP 800-53 Revision 4 (v4): CP-2 (5)
NIST: NIST SP 800-53A (v1): CP-2 (5).1 (a)

---

**CCI:** CCI-000482 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization plans for the continuance of essential business functions with little or no loss of operational continuity.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-2 (5)
NIST: NIST SP 800-53 Revision 4 (v4): CP-2 (5)
NIST: NIST SP 800-53A (v1): CP-2 (5).1 (a)

---

**CCI:** CCI-001601 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2010-05-12

**Definition:** The organization sustains operational continuity of essential missions at alternate processing and/or storage sites until information system restoration at primary processing and/or storage sites.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-2 (6)
NIST: NIST SP 800-53 Revision 4 (v4): CP-2 (6)
NIST: NIST SP 800-53A (v1): CP-2 (6).1 (ii)

---

**CCI:** CCI-001602 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2010-05-12

**Definition:** The organization sustains operational continuity of essential business functions at alternate processing and/or storage sites until information system restoration at primary processing and/or storage sites.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-2 (6)
NIST: NIST SP 800-53 Revision 4 (v4): CP-2 (6)
NIST: NIST SP 800-53A (v1): CP-2 (6).1 (ii)

---

**CCI:** CCI-000483 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization plans for the transfer of essential missions to alternate processing and/or storage sites with little or no loss of operational continuity.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-2 (6)
NIST: NIST SP 800-53 Revision 4 (v4): CP-2 (6)
NIST: NIST SP 800-53A (v1): CP-2 (6).1 (i)

**CCI:** CCI-000484 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-18
**Definition:** The organization plans for the transfer of essential business functions to alternate processing and/or storage sites with little or no loss of operational continuity.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CP-2 (6)
NIST: NIST SP 800-53 Revision 4 (v4): CP-2 (6)
NIST: NIST SP 800-53A (v1): CP-2 (6).1 (i)

**CCI:** CCI-002827 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-07-20
**Definition:** The organization coordinates its contingency plan with the contingency plans of external service providers to ensure that contingency requirements can be satisfied.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): CP-2 (7)

**CCI:** CCI-002828 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-07-20
**Definition:** The organization identifies critical information system assets supporting essential missions.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): CP-2 (8)

**CCI:** CCI-002829 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-07-20
**Definition:** The organization identifies critical information system assets supporting essential business functions.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): CP-2 (8)

**CCI:** CCI-000486 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization provides contingency training to information system users consistent with assigned roles and responsibilities within an organization-defined time period of assuming a contingency role or responsibility.
**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-3
NIST: NIST SP 800-53 Revision 4 (v4): CP-3 a
NIST: NIST SP 800-53A (v1): CP-3.1 (i)

---

**CCI:** CCI-002833 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-07-20
**Definition:** The organization defines the time period that contingency training is to be provided to information system users consistent with assigned roles and responsibilities within assuming a contingency role or responsibility.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): CP-3 a

---

**CCI:** CCI-002834 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-07-20
**Definition:** The organization provides contingency training to information system users consistent with assigned roles and responsibilities when required by information system changes.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): CP-3 b

---

**CCI:** CCI-000485 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization defines the frequency of refresher contingency training to information system users.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CP-3
NIST: NIST SP 800-53 Revision 4 (v4): CP-3 c
NIST: NIST SP 800-53A (v1): CP-3.1 (ii)

---

**CCI:** CCI-000487 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization provides refresher contingency training to information system users consistent with assigned roles and responsibilities in accordance with organization-defined frequency.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CP-3
NIST: NIST SP 800-53 Revision 4 (v4): CP-3 c
NIST: NIST SP 800-53A (v1): CP-3.1 (iii)

---

**CCI:** CCI-000488 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-3 (1)
NIST: NIST SP 800-53 Revision 4 (v4): CP-3 (1)
NIST: NIST SP 800-53A (v1): CP-3 (1).1 (i) (ii)

---

**CCI:** CCI-000489 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization employs automated mechanisms to provide a more thorough and realistic contingency training environment.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-3 (2)
NIST: NIST SP 800-53 Revision 4 (v4): CP-3 (2)
NIST: NIST SP 800-53A (v1): CP-3 (2).1

---

**CCI:** CCI-000490 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization defines the frequency with which to test the contingency plan for the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-4
NIST: NIST SP 800-53 Revision 4 (v4): CP-4 a
NIST: NIST SP 800-53A (v1): CP-4.1 (ii)

---

**CCI:** CCI-000492 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization defines contingency plan tests to be conducted for the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-4
NIST: NIST SP 800-53 Revision 4 (v4): CP-4 a
NIST: NIST SP 800-53A (v1): CP-4.1 (i)

---

**CCI:** CCI-000494 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization tests the contingency plan for the information system in accordance with organization-defined frequency using organization-defined tests to determine the effectiveness of the plan and the organizational readiness to execute the plan.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-4 a

NIST: NIST SP 800-53 Revision 4 (v4): CP-4 a
NIST: NIST SP 800-53A (v1): CP-4.1 (iii)

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000496 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization reviews the contingency plan test results. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CP-4 b<br>NIST: NIST SP 800-53 Revision 4 (v4): CP-4 b<br>NIST: NIST SP 800-53A (v1): CP-4.1 (iv) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000497 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization initiates corrective actions, if needed, after reviewing the contingency plan test results. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CP-4 b<br>NIST: NIST SP 800-53 Revision 4 (v4): CP-4 c<br>NIST: NIST SP 800-53A (v1): CP-4.1 (iv) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000498 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization coordinates contingency plan testing with organizational elements responsible for related plans. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CP-4 (1)<br>NIST: NIST SP 800-53 Revision 4 (v4): CP-4 (1)<br>NIST: NIST SP 800-53A (v1): CP-4 (1).1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000500 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization tests the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CP-4 (2)<br>NIST: NIST SP 800-53 Revision 4 (v4): CP-4 (2) (a)<br>NIST: NIST SP 800-53A (v1): CP-4 (2).1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002835 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published** | 2013-07-20 |

**Date:**

**Definition:** The organization tests the contingency plan at the alternate processing site to evaluate the capabilities of the alternate processing site to support contingency operations.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CP-4 (2) (b)

---

**CCI:** CCI-000502 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization employs automated mechanisms to more thoroughly and effectively test the contingency plan.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-4 (3)
NIST: NIST SP 800-53 Revision 4 (v4): CP-4 (3)
NIST: NIST SP 800-53A (v1): CP-4 (3).1

---

**CCI:** CCI-000504 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization includes a full recovery and reconstitution of the information system to a known state as part of contingency plan testing.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-4 (4)
NIST: NIST SP 800-53 Revision 4 (v4): CP-4 (4)4
NIST: NIST SP 800-53A (v1): CP-4 (4).1

---

**CCI:** CCI-000505 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-6
NIST: NIST SP 800-53 Revision 4 (v4): CP-6 a
NIST: NIST SP 800-53A (v1): CP-6.1 (i)

---

**CCI:** CCI-002836 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-20

**Definition:** The organization ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CP-6 b

---

**CCI:** CCI-000507
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2009-09-21
**Definition:** The organization identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CP-6 (1)
NIST: NIST SP 800-53 Revision 4 (v4): CP-6 (1)
NIST: NIST SP 800-53A (v1): CP-6 (1).1 (ii)

---

**CCI:** CCI-000508
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2009-09-21
**Definition:** The organization configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CP-6 (2)
NIST: NIST SP 800-53 Revision 4 (v4): CP-6 (2)
NIST: NIST SP 800-53A (v1): CP-6 (2).1

---

**CCI:** CCI-001604
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2010-05-12
**Definition:** The organization outlines explicit mitigation actions for organization identified accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CP-6 (3)
NIST: NIST SP 800-53 Revision 4 (v4): CP-6 (3)
NIST: NIST SP 800-53A (v1): CP-6 (3).1 (ii)

---

**CCI:** CCI-000509
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2009-09-21
**Definition:** The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CP-6 (3)
NIST: NIST SP 800-53 Revision 4 (v4): CP-6 (3)
NIST: NIST SP 800-53A (v1): CP-6 (3).1 (i)

---

**CCI:** CCI-000510
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2009-09-21
**Definition:** The organization defines the time period consistent with recovery time and recovery point

objectives for essential missions/business functions to permit the transfer and resumption of organization-defined information system operations at an alternate processing site when the primary processing capabilities are unavailable.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-7
NIST: NIST SP 800-53 Revision 4 (v4): CP-7 a
NIST: NIST SP 800-53A (v1): CP-7.1 (ii)

---

**CCI:** CCI-000513 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization establishes an alternate processing site including necessary agreements to permit the transfer and resumption of organization-defined information system operations for essential missions within an organization-defined time period consistent with recovery time and recovery point objectives when the primary processing capabilities are unavailable.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-7 a
NIST: NIST SP 800-53 Revision 4 (v4): CP-7 a
NIST: NIST SP 800-53A (v1): CP-7.1 (iii)

---

**CCI:** CCI-000514 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization establishes an alternate processing site including necessary agreements to permit the transfer and resumption of organization-defined information system operations for essential business functions within an organization-defined time period consistent with recovery time and recovery point objectives when the primary processing capabilities are unavailable.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-7 a
NIST: NIST SP 800-53 Revision 4 (v4): CP-7 a
NIST: NIST SP 800-53A (v1): CP-7.1 (iii)

---

**CCI:** CCI-002839 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-20

**Definition:** The organization defines information system operations that are permitted to transfer and resume at an alternate processing site for essential missions/business functions when the primary processing capabilities are unavailable.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CP-7 a

---

**CCI:** CCI-000515 **Status:** draft

**Contributor:** DISA FSO **Published** 2009-09-21

**Date:**

**Definition:** The organization ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-7 b
NIST: NIST SP 800-53 Revision 4 (v4): CP-7 b
NIST: NIST SP 800-53A (v1): CP-7.1 (iv)

---

**CCI:** CCI-000521 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-7 (5)
NIST: NIST SP 800-53 Revision 4 (v4): CP-7 c
NIST: NIST SP 800-53A (v1): CP-7 (5).1

---

**CCI:** CCI-000516 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization identifies an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-7 (1)
NIST: NIST SP 800-53 Revision 4 (v4): CP-7 (1)
NIST: NIST SP 800-53A (v1): CP-7 (1).1 (ii)

---

**CCI:** CCI-001606 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2010-05-12

**Definition:** The organization outlines explicit mitigation actions for organization-identified potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-7 (2)
NIST: NIST SP 800-53 Revision 4 (v4): CP-7 (2)
NIST: NIST SP 800-53A (v1): CP-7 (2).1 (ii)

---

**CCI:** CCI-000517 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-7 (2)
NIST: NIST SP 800-53 Revision 4 (v4): CP-7 (2)
NIST: NIST SP 800-53A (v1): CP-7 (2).1 (i)

---

**CCI:** CCI-000518 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with the organizational availability requirements (including recovery time objectives).

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-7 (3)
NIST: NIST SP 800-53 Revision 4 (v4): CP-7 (3)
NIST: NIST SP 800-53A (v1): CP-7 (3).1

---

**CCI:** CCI-000519 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization prepares the alternate processing site so that it is ready to be used as the operational site supporting essential missions.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-7 (4)
NIST: NIST SP 800-53 Revision 4 (v4): CP-7 (4)
NIST: NIST SP 800-53A (v1): CP-7 (4).1

---

**CCI:** CCI-000520 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization prepares the alternate processing site so that it is ready to be used as the operational site supporting essential business functions.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-7 (4)
NIST: NIST SP 800-53 Revision 4 (v4): CP-7 (4)
NIST: NIST SP 800-53A (v1): CP-7 (4).1

---

**CCI:** CCI-002837 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-20

**Definition:** The organization plans for circumstances that preclude returning to the primary processing site.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CP-7 (6)

---

**CCI:** CCI-002838 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-20

**Definition:** The organization prepares for circumstances that preclude returning to the primary processing site.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CP-7 (6)

---

**CCI:** CCI-000522 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization defines the time period within which to permit the resumption of organization-defined information system operations for essential missions when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-8

NIST: NIST SP 800-53 Revision 4 (v4): CP-8

NIST: NIST SP 800-53A (v1): CP-8.1 (ii)

---

**CCI:** CCI-000523 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization defines the time period within which to permit the resumption of organization-defined information system operations for essential business functions when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-8

NIST: NIST SP 800-53 Revision 4 (v4): CP-8

NIST: NIST SP 800-53A (v1): CP-8.1 (ii)

---

**CCI:** CCI-000524 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization establishes alternate telecommunication services including necessary agreements to permit the resumption of organization-defined information system operations for essential missions within an organization-defined time period when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-8

NIST: NIST SP 800-53 Revision 4 (v4): CP-8

NIST: NIST SP 800-53A (v1): CP-8.1 (iii)

---

**CCI:** CCI-000525 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization establishes alternate telecommunication services including necessary agreements to permit the resumption of organization-defined information system operations for essential business functions within an organization-defined time period when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-8

NIST: NIST SP 800-53 Revision 4 (v4): CP-8

NIST: NIST SP 800-53A (v1): CP-8.1 (iii)

---

**CCI:** CCI-002840 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-20

**Definition:** The organization defines the information system operations to be resumed for essential missions within the organization-defined time period when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CP-8

---

**CCI:** CCI-002841 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-20

**Definition:** The organization defines the information system operations to be resumed for essential business functions within the organization-defined time period when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CP-8

---

**CCI:** CCI-000526 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization develops primary telecommunications service agreements that contain priority-of-service provisions in accordance with the organization's availability requirements (including recovery time objectives).

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-8 (1) (a)

NIST: NIST SP 800-53 Revision 4 (v4): CP-8 (1) (a)

NIST: NIST SP 800-53A (v1): CP-8 (1).1 (i)

---

**CCI:** CCI-000527 **Status:** draft

**Contributor:** DISA FSO **Published** 2009-09-21

**Date:**

**Definition:** The organization develops alternate telecommunications service agreements that contain priority-of-service provisions in accordance with the organization's availability requirements (including recovery time objectives).

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-8 (1) (a)
NIST: NIST SP 800-53 Revision 4 (v4): CP-8 (1) (a)
NIST: NIST SP 800-53A (v1): CP-8 (1).1 (i)

---

**CCI:** CCI-000528 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary telecommunications services are provided by a common carrier.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-8 (1) (b)
NIST: NIST SP 800-53 Revision 4 (v4): CP-8 (1) (b)
NIST: NIST SP 800-53A (v1): CP-8 (1).1 (ii)

---

**CCI:** CCI-000529 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the alternate telecommunications services are provided by a common carrier.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-8 (1) (b)
NIST: NIST SP 800-53 Revision 4 (v4): CP-8 (1) (b)
NIST: NIST SP 800-53A (v1): CP-8 (1).1 (ii)

---

**CCI:** CCI-000530 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization obtains alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-8 (2)
NIST: NIST SP 800-53 Revision 4 (v4): CP-8 (2)
NIST: NIST SP 800-53A (v1): CP-8 (2).1

---

**CCI:** CCI-000531 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

| | | | |
|---|---|---|---|
| **Definition:** | The organization obtains alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CP-8 (3)<br>NIST: NIST SP 800-53 Revision 4 (v4): CP-8 (3)<br>NIST: NIST SP 800-53A (v1): CP-8 (3).1 (ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000532 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization requires primary telecommunications service providers to have contingency plans. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CP-8 (4)<br>NIST: NIST SP 800-53 Revision 4 (v4): CP-8 (4) (a)<br>NIST: NIST SP 800-53A (v1): CP-8 (4).1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000533 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization requires alternate telecommunications service providers to have contingency plans. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CP-8 (4)<br>NIST: NIST SP 800-53 Revision 4 (v4): CP-8 (4) (a)<br>NIST: NIST SP 800-53A (v1): CP-8 (4).1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002842 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-20 |
| **Definition:** | The organization reviews provider contingency plans to ensure that the plans meet organizational contingency requirements. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CP-8 (4) (b) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002843 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-20 |
| **Definition:** | The organization defines the frequency with which to obtain evidence of contingency testing by providers. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CP-8 (4) (c) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002844 | **Status:** | draft |

| | | | |
|---|---|---|---|
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-20 |
| **Definition:** | The organization defines the frequency with which to obtain evidence of contingency training by providers. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CP-8 (4) (c) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002845 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-20 |
| **Definition:** | The organization obtains evidence of contingency testing by providers in accordance with organization-defined frequency. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CP-8 (4) (c) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002846 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-20 |
| **Definition:** | The organization obtains evidence of contingency training by providers in accordance with organization-defined frequency. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CP-8 (4) (c) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002847 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-20 |
| **Definition:** | The organization defines the frequency with which to test alternate telecommunication services. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CP-8 (5) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002848 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-20 |
| **Definition:** | The organization tests alternate telecommunication services per organization-defined frequency. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CP-8 (5) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000534 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization defines the frequency of conducting user-level information backups to support recovery time objectives and recovery point objectives. | | |
| **Type:** | policy | | |

**References:** NIST: NIST SP 800-53 (v3): CP-9 (a)
NIST: NIST SP 800-53 Revision 4 (v4): CP-9 (a)
NIST: NIST SP 800-53A (v1): CP-9 (6).1 (ii)

---

**CCI:** CCI-000535 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization conducts backups of user-level information contained in the information system per organization-defined frequency that is consistent with recovery time and recovery point objectives.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CP-9 (a)
NIST: NIST SP 800-53 Revision 4 (v4): CP-9 (a)
NIST: NIST SP 800-53A (v1): CP-9.1 (iv)

---

**CCI:** CCI-000536 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization defines the frequency of conducting system-level information backups to support recovery time objectives and recovery point objectives.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CP-9 (b)
NIST: NIST SP 800-53 Revision 4 (v4): CP-9 (b)
NIST: NIST SP 800-53A (v1): CP-9.1 (ii)

---

**CCI:** CCI-000537 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization conducts backups of system-level information contained in the information system per organization-defined frequency that is consistent with recovery time and recovery point objectives.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CP-9 (b)
NIST: NIST SP 800-53 Revision 4 (v4): CP-9 (b)
NIST: NIST SP 800-53A (v1): CP-9.1 (v)

---

**CCI:** CCI-000538 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization defines the frequency of conducting information system documentation backups, including security-related documentation, to support recovery time objectives and recovery point objectives.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CP-9 (c)
NIST: NIST SP 800-53 Revision 4 (v4): CP-9 (c)

NIST: NIST SP 800-53A (v1): CP-9.1 (iii)

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000539 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization conducts backups of information system documentation, including security-related documentation, per an organization-defined frequency that is consistent with recovery time and recovery point objectives. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CP-9 (c)<br>NIST: NIST SP 800-53 Revision 4 (v4): CP-9 (c)<br>NIST: NIST SP 800-53A (v1): CP-9.1 (vi) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000540 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization protects the confidentiality, integrity, and availability of backup information at storage locations. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CP-9 (d)<br>NIST: NIST SP 800-53 Revision 4 (v4): CP-9 (d)<br>NIST: NIST SP 800-53A (v1): CP-9.2 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000541 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization defines the frequency with which to test backup information to verify media reliability and information integrity. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CP-9 (1)<br>NIST: NIST SP 800-53 Revision 4 (v4): CP-9 (1)<br>NIST: NIST SP 800-53A (v1): CP-9 (1).1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000542 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization tests backup information per an organization-defined frequency to verify media reliability and information integrity. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CP-9 (1)<br>NIST: NIST SP 800-53 Revision 4 (v4): CP-9 (1)<br>NIST: NIST SP 800-53A (v1): CP-9 (1).1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000543 | **Status:** | draft |

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization uses a sample of backup information in the restoration of selected information system functions as part of contingency plan testing.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-9 (2)
NIST: NIST SP 800-53 Revision 4 (v4): CP-9 (2)
NIST: NIST SP 800-53A (v1): CP-9 (2).1

---

**CCI:** CCI-002849 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-20

**Definition:** The organization defines critical information system software and other security-related information, of which backup copies must be stored in a separate facility or in a fire-rated container.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CP-9 (3)

---

**CCI:** CCI-002850 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-20

**Definition:** The organization stores backup copies of organization-defined critical information system software and other security-related information in a separate facility or in a fire-rated container that is not collocated with the operational system.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CP-9 (3)

---

**CCI:** CCI-000547 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization defines the time period and transfer rate of the information system backup information to the alternate storage site consistent with the recovery time and recovery point objectives.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-9 (5)
NIST: NIST SP 800-53 Revision 4 (v4): CP-9 (5)
NIST: NIST SP 800-53A (v1): CP-9 (5).1 (i)

---

**CCI:** CCI-000548 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization transfers information system backup information to the alternate storage site in accordance with the organization-defined time period and transfer rate consistent with the recovery time and recovery point objectives.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-9 (5)
NIST: NIST SP 800-53 Revision 4 (v4): CP-9 (5)
NIST: NIST SP 800-53A (v1): CP-9 (5).1 (ii)

---

**CCI:** CCI-001609 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2010-05-12
**Definition:** The organization can activate the redundant secondary information system that is not collocated with the primary system without loss of information or disruption to operations.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CP-9 (6)
NIST: NIST SP 800-53 Revision 4 (v4): CP-9 (6)
NIST: NIST SP 800-53A (v1): CP-9 (6).1 (ii)

---

**CCI:** CCI-000549 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization maintains a redundant secondary information system that is not collocated with the primary system.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CP-9 (6)
NIST: NIST SP 800-53 Revision 4 (v4): CP-9 (6)
NIST: NIST SP 800-53A (v1): CP-9 (6).1 (i)

---

**CCI:** CCI-002851 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-07-20
**Definition:** The organization defines the backup information that requires dual authorization for deletion or destruction.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): CP-9 (7)

---

**CCI:** CCI-002852 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-07-20
**Definition:** The organization enforces dual authorization for the deletion or destruction of organization-defined backup information.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): CP-9 (7)

---

**CCI:** CCI-000550 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization provides for the recovery and reconstitution of the information system to a

known state after a disruption.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-10
NIST: NIST SP 800-53 Revision 4 (v4): CP-10
NIST: NIST SP 800-53A (v1): CP-10.1

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000551 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |

**Definition:** The organization provides for the recovery and reconstitution of the information system to a known state after a compromise.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-10
NIST: NIST SP 800-53 Revision 4 (v4): CP-10
NIST: NIST SP 800-53A (v1): CP-10.1

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000552 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |

**Definition:** The organization provides for the recovery and reconstitution of the information system to a known state after a failure.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-10
NIST: NIST SP 800-53 Revision 4 (v4): CP-10
NIST: NIST SP 800-53A (v1): CP-10.1

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000553 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |

**Definition:** The information system implements transaction recovery for systems that are transaction-based.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-10 (2)
NIST: NIST SP 800-53 Revision 4 (v4): CP-10 (2)
NIST: NIST SP 800-53A (v1): CP-10 (2).1

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000556 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |

**Definition:** The organization defines restoration time periods within which to restore information system components from configuration-controlled and integrity-protected information representing a known, operational state for the components.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-10 (4)

NIST: NIST SP 800-53 Revision 4 (v4): CP-10 (4)
NIST: NIST SP 800-53A (v1): CP-10 (4).1

---

**CCI:** CCI-000557 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization provides the capability to restore information system components within organization-defined restoration time periods from configuration-controlled and integrity-protected information representing a known, operational state for the components.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CP-10 (4)
NIST: NIST SP 800-53 Revision 4 (v4): CP-10 (4)
NIST: NIST SP 800-53A (v1): CP-10 (4).1

---

**CCI:** CCI-000560 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization protects backup and restoration hardware.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CP-10 (6)
NIST: NIST SP 800-53 Revision 4 (v4): CP-10 (6)
NIST: NIST SP 800-53A (v1): CP-10 (6).1

---

**CCI:** CCI-000561 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization protects backup and restoration firmware.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CP-10 (6)
NIST: NIST SP 800-53 Revision 4 (v4): CP-10 (6)
NIST: NIST SP 800-53A (v1): CP-10 (6).1

---

**CCI:** CCI-000562 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization protects backup and restoration software.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CP-10 (6)
NIST: NIST SP 800-53 Revision 4 (v4): CP-10 (6)
NIST: NIST SP 800-53A (v1): CP-10 (6).1

---

**CCI:** CCI-002853 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-07-20

**Definition:** The information system provides the capability to employ organization-defined alternative communications protocols in support of maintaining continuity of operations.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CP-11

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002854 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-20 |

**Definition:** The organization defines the alternative communications protocols the information system must be capable of providing in support of maintaining continuity of operations.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CP-11

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002855 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-20 |

**Definition:** The information system, when organization-defined conditions are detected, enters a safe mode of operation with organization-defined restrictions of safe mode of operation.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CP-12

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002856 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-20 |

**Definition:** The organization defines the conditions that, when detected, the information system enters a safe mode of operation with organization-defined restrictions of safe mode of operation.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CP-12

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002857 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-20 |

**Definition:** The organization defines the restrictions of the safe mode of operation that the information system will enter when organization-defined conditions are detected.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CP-12

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002858 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-20 |

**Definition:** The organization employs organization-defined alternative or supplemental security mechanisms for satisfying organization-defined security functions when the primary means of implementing the security function is unavailable or compromised.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): CP-13

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002859 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-20 |
| **Definition:** | The organization defines the alternative or supplemental security mechanisms that will be employed for satisfying organization-defined security functions when the primary means of implementing the security function is unavailable or compromised. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CP-13 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002860 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-20 |
| **Definition:** | The organization defines the security functions that must be satisfied when the primary means of implementing the security function is unavailable or compromised. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): CP-13 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003463 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-07 |
| **Definition:** | The organization confirms to the greatest extent practicable upon collection or creation of personally identifiable information (PII), the accuracy of that information. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): DI-1 a | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003464 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-07 |
| **Definition:** | The organization confirms to the greatest extent practicable upon collection or creation of personally identifiable information (PII), the relevancy of that information. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): DI-1 a | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003465 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-07 |
| **Definition:** | The organization confirms to the greatest extent practicable upon collection or creation of personally identifiable information (PII), the timeliness of that information. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): DI-1 a | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003466 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-07 |

**Definition:** The organization confirms to the greatest extent practicable upon collection or creation of personally identifiable information (PII), the completeness of that information.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): DI-1 a

---

**CCI:** CCI-003467 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

**Definition:** The organization collects personally identifiable information (PII) directly from the individual to the greatest extent practicable.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): DI-1 b

---

**CCI:** CCI-003468 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

**Definition:** The organization defines the frequency on which it will check for, and correct as necessary, inaccurate or outdated personally identifiable information (PII) used by its programs or systems.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): DI-1 c

---

**CCI:** CCI-003469 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

**Definition:** The organization checks for, and corrects as necessary, any inaccurate or outdated personally identifiable information (PII) used by its programs or systems on an organization-defined frequency.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): DI-1 c

---

**CCI:** CCI-003470 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

**Definition:** The organization issues guidelines ensuring the quality of disseminated Privacy Act information.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): DI-1 d

---

**CCI:** CCI-003471 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

**Definition:** The organization issues guidelines ensuring the utility of disseminated Privacy Act information.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): DI-1 d

---

**CCI:** CCI-003472 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

**Definition:** The organization issues guidelines ensuring the objectivity of disseminated Privacy Act information.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): DI-1 d

---

**CCI:** CCI-003473 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

**Definition:** The organization issues guidelines ensuring the integrity of disseminated Privacy Act information.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): DI-1 d

---

**CCI:** CCI-003474 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

**Definition:** The organization issues guidelines maximizing the quality of disseminated Privacy Act information.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): DI-1 d

---

**CCI:** CCI-003475 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

**Definition:** The organization issues guidelines maximizing the utility of disseminated Privacy Act information.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): DI-1 d

---

**CCI:** CCI-003476 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

**Definition:** The organization issues guidelines maximizing the objectivity of disseminated Privacy Act information.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): DI-1 d

---

**CCI:** CCI-003477 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

**Definition:** The organization issues guidelines maximizing the integrity of disseminated Privacy Act information.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): DI-1 d

---

**CCI:** CCI-003478 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

**Definition:** The organization requests the individual or individual's authorized representative validate personally identifiable information (PII) during the collection process.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): DI-1 (1)

---

**CCI:** CCI-003479 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

**Definition:** The organization defines the frequency on which it will request the individual, or individual's authorized representative, revalidate that personally identifiable information (PII) collected is still accurate.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): DI-1 (2)

---

**CCI:** CCI-003480 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

**Definition:** On an organization-defined frequency, the organization requests the individual, or individual's authorized representative, revalidate that personally identifiable information (PII) collected is still accurate.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): DI-1 (2)

---

**CCI:** CCI-003481 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

**Definition:** The organization documents processes to ensure the integrity of personally identifiable information (PII) through existing security controls.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): DI-2 a

---

**CCI:** CCI-003482 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-07

**Definition:** The organization, when appropriate, establishes a Data Integrity Board.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): DI-2 b

**CCI:** CCI-003483 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-11-07
**Definition:** The organization's Data Integrity Board oversees the organizational Computer Matching Agreements.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): DI-2 b

---

**CCI:** CCI-003484 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-11-07
**Definition:** The organization's Data Integrity Board ensures the Computer Matching Agreements comply with the computer matching provisions of the Privacy Act.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): DI-2 b

---

**CCI:** CCI-003485 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-11-07
**Definition:** The organization publishes Computer Matching Agreements on its public website.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): DI-2 (1)

---

**CCI:** CCI-003486 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-11-08
**Definition:** The organization identifies the minimum personally identifiable information (PII) elements that are relevant and necessary to accomplish the legally authorized purpose of collection.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): DM-1 a

---

**CCI:** CCI-003487 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-11-08
**Definition:** The organization limits the collection and retention of personally identifiable information (PII) to the minimum elements identified for the purposes described in the published privacy notice.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): DM-1 b

---

**CCI:** CCI-003488 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-11-08
**Definition:** The organization limits the collection and retention of personally identifiable information

| | | | |
|---|---|---|---|
| | (PII) to the minimum elements identified for the purposes which the individual has provided consent. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): DM-1 b | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003489 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-08 |
| **Definition:** | The organization defines the frequency, minimally annually, for conducting reviews of its personally identifiable information (PII) holdings. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): DM-1 c | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003490 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-08 |
| **Definition:** | The organization conducts an initial evaluation of personally identifiable information (PII) holdings. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): DM-1 c | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003491 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-08 |
| **Definition:** | The organization establishes a schedule for regularly reviewing the personally identifiable information (PII) holdings on an organization-defined frequency to ensure that only PII identified in the notice is collected and retained. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): DM-1 c | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003492 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-08 |
| **Definition:** | The organization follows a schedule for regularly reviewing the personally identifiable information (PII) holdings on an organization-defined frequency to ensure that only PII identified in the notice is collected and retained. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): DM-1 c | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003493 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-08 |
| **Definition:** | The organization establishes a schedule for regularly reviewing the personally identifiable information (PII) holdings on an organization-defined frequency to ensure the PII continues to be necessary to accomplish the legally authorized purpose. | | |

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): DM-1 c

---

**CCI:** CCI-003494 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-08

**Definition:** The organization follows a schedule for regularly reviewing the personally identifiable information (PII) holdings on an organization-defined frequency to ensure the PII continues to be necessary to accomplish the legally authorized purpose.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): DM-1 c

---

**CCI:** CCI-003495 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-08

**Definition:** The organization, where feasible and within the limits of technology, locates and removes/redacts specified personally identifiable information (PII).

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): DM-1 (1)

---

**CCI:** CCI-003496 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-08

**Definition:** The organization, where feasible and within the limits of technology, uses anonymization and de-identification techniques to permit use of the retained Privacy Act information while reducing its sensitivity and reducing the risk resulting from disclosure.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): DM-1 (1)

---

**CCI:** CCI-003497 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-08

**Definition:** The organization defines the time period for retaining each collection of personally identifiable information (PII) that is required to fulfill the purpose(s) identified in the published privacy notice or required by law.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): DM-2 a

---

**CCI:** CCI-003498 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-08

**Definition:** The organization retains each collection of personally identifiable information (PII) for the organization-defined time period to fulfill the purpose(s) identified in the published privacy notice or as required by law.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): DM-2 a

---

**CCI:** CCI-003499 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-08

**Definition:** The organization disposes of, destroys, erases, and/or anonymizes the personally identifiable information (PII), regardless of the method of storage, in accordance with a NARA-approved record retention schedule.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): DM-2 b

---

**CCI:** CCI-003500 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-08

**Definition:** The organization disposes of, destroys, erases, and/or anonymizes the personally identifiable information (PII), regardless of the method of storage, in a manner that prevents loss, theft, misuse, or unauthorized access.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): DM-2 b

---

**CCI:** CCI-003501 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-08

**Definition:** The organization defines the techniques or methods to be employed to ensure the secure deletion or destruction of personally identifiable information (PII) (including originals, copies, and archived records).

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): DM-2 c

---

**CCI:** CCI-003502 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-08

**Definition:** The organization uses organization-defined techniques or methods to ensure secure deletion or destruction of personally identifiable information (PII) (including originals, copies, and archived records).

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): DM-2 c

---

**CCI:** CCI-003503 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-08

**Definition:** The organization, where feasible, configures its information systems to record the date personally identifiable information (PII) is collected, created, or updated.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): DM-2 (1)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003504 | **Status:** | deprecated |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-08 |
| **Definition:** | The organization, where feasible, configures its information systems to record the date personally identifiable information (PII) is created. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): DM-2 (1) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003505 | **Status:** | deprecated |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-08 |
| **Definition:** | The organization, where feasible, configures its information systems to record the date personally identifiable information (PII) is updated. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): DM-2 (1) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003506 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-08 |
| **Definition:** | The organization, where feasible, configures its information systems to record when personally identifiable information (PII) is to be deleted or archived under an approved record retention schedule. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): DM-2 (1) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003507 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-08 |
| **Definition:** | The organization develops policies that minimize the use of personally identifiable information (PII) for testing. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): DM-3 a | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003508 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-08 |
| **Definition:** | The organization develops policies that minimize the use of personally identifiable information (PII) for training. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): DM-3 a | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003509 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-08 |

| | | | |
|---|---|---|---|
| **Definition:** | The organization develops policies that minimize the use of personally identifiable information (PII) for research. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): DM-3 a | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003510 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-08 |
| **Definition:** | The organization develops procedures that minimize the use of personally identifiable information (PII) for testing. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): DM-3 a | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003511 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-08 |
| **Definition:** | The organization develops procedures that minimize the use of personally identifiable information (PII) for training. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): DM-3 a | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003512 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-08 |
| **Definition:** | The organization develops procedures that minimize the use of personally identifiable information (PII) for research. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): DM-3 a | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003513 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-08 |
| **Definition:** | The organization implements controls to protect personally identifiable information (PII) used for testing. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): DM-3 b | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003514 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-08 |
| **Definition:** | The organization implements controls to protect personally identifiable information (PII) used for training. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): DM-3 b | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003515 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-08 |
| **Definition:** | The organization implements controls to protect personally identifiable information (PII) used for research. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): DM-3 b | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003516 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-08 |
| **Definition:** | The organization, where feasible, uses techniques to minimize the risk to privacy of using personally identifiable information (PII) for research. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): DM-3 (1) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003517 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-08 |
| **Definition:** | The organization, where feasible, uses techniques to minimize the risk to privacy of using personally identifiable information (PII) for testing. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): DM-3 (1) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003518 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-08 |
| **Definition:** | The organization, where feasible, uses techniques to minimize the risk to privacy of using personally identifiable information (PII) for training. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): DM-3 (1) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000756 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |
| **Definition:** | The organization develops an identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): IA-1 a<br>NIST: NIST SP 800-53 Revision 4 (v4): IA-1 a 1<br>NIST: NIST SP 800-53A (v1): IA-1.1 (i) (ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000757 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published** | 2009-09-17 |

**Date:**

**Definition:** The organization disseminates to organization-defined personnel or roles an identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): IA-1 a
NIST: NIST SP 800-53 Revision 4 (v4): IA-1 a 1
NIST: NIST SP 800-53A (v1): IA-1.1 (iii)

---

**CCI:** CCI-000760 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-17

**Definition:** The organization develops procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): IA-1 b
NIST: NIST SP 800-53 Revision 4 (v4): IA-1 a 2
NIST: NIST SP 800-53A (v1): IA-1.1 (v)

---

**CCI:** CCI-000761 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-17

**Definition:** The organization disseminates to organization-defined personnel or roles procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): IA-1 b
NIST: NIST SP 800-53 Revision 4 (v4): IA-1 a 2
NIST: NIST SP 800-53A (v1): IA-1.1 (vi)

---

**CCI:** CCI-001932 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-05-03

**Definition:** The organization documents an identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-1 a 1

---

**CCI:** CCI-001933 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-05-03

**Definition:** The organization defines the personnel or roles to be recipients of the identification and authentication policy and the procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.

| | | | |
|---|---|---|---|
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IA-1 a 1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001934 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |
| **Definition:** | The organization documents procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IA-1 a 2 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000758 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |
| **Definition:** | The organization reviews and updates identification and authentication policy in accordance with the organization-defined frequency. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): IA-1 a<br>NIST: NIST SP 800-53 Revision 4 (v4): IA-1 b 1<br>NIST: NIST SP 800-53A (v1): IA-1.2 (ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000759 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |
| **Definition:** | The organization defines a frequency for reviewing and updating the identification and authentication policy. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): IA-1 a<br>NIST: NIST SP 800-53 Revision 4 (v4): IA-1 b 1<br>NIST: NIST SP 800-53A (v1): IA-1.2 (i) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000762 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |
| **Definition:** | The organization reviews and updates identification and authentication procedures in accordance with the organization-defined frequency. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): IA-1 b<br>NIST: NIST SP 800-53 Revision 4 (v4): IA-1 b 2<br>NIST: NIST SP 800-53A (v1): IA-1.2 (iv) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000763 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |

**Definition:** The organization defines a frequency for reviewing and updating the identification and authentication procedures.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): IA-1 b
NIST: NIST SP 800-53 Revision 4 (v4): IA-1 b 2
NIST: NIST SP 800-53A (v1): IA-1.2 (iii)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000764 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |

**Definition:** The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): IA-2
NIST: NIST SP 800-53 Revision 4 (v4): IA-2
NIST: NIST SP 800-53A (v1): IA-2.1

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000765 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |

**Definition:** The information system implements multifactor authentication for network access to privileged accounts.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): IA-2 (1)
NIST: NIST SP 800-53 Revision 4 (v4): IA-2 (1)
NIST: NIST SP 800-53A (v1): IA-2 (1).1

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000766 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |

**Definition:** The information system implements multifactor authentication for network access to non-privileged accounts.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): IA-2 (2)
NIST: NIST SP 800-53 Revision 4 (v4): IA-2 (2)
NIST: NIST SP 800-53A (v1): IA-2 (2).1

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000767 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |

**Definition:** The information system implements multifactor authentication for local access to privileged accounts.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): IA-2 (3)

| | | | |
|---|---|---|---|
| | NIST: NIST SP 800-53 Revision 4 (v4): IA-2 (3)<br>NIST: NIST SP 800-53A (v1): IA-2 (3).1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000768 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |
| **Definition:** | The information system implements multifactor authentication for local access to non-privileged accounts. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): IA-2 (4)<br>NIST: NIST SP 800-53 Revision 4 (v4): IA-2 (4)<br>NIST: NIST SP 800-53A (v1): IA-2 (4).1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000770 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |
| **Definition:** | The organization requires individuals to be authenticated with an individual authenticator when a group authenticator is employed. | | |
| **Type:** | policy, technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): IA-2 (5) (b)<br>NIST: NIST SP 800-53 Revision 4 (v4): IA-2 (5)<br>NIST: NIST SP 800-53A (v1): IA-2 (5).2 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001935 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |
| **Definition:** | The organization defines the strength of mechanism requirements for the device that is separate from the system gaining access to privileged accounts. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IA-2 (6) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001936 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |
| **Definition:** | The information system implements multifactor authentication for network access to privileged accounts such that one of the factors is provided by a device separate from the system gaining access. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IA-2 (6) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001937 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |
| **Definition:** | The device used in the information system implementation of multifactor authentication for network access to privileged accounts meets organization-defined strength of mechanism | | |

| | | | |
|---|---|---|---|
| | requirements. | | |
| **Type:** | technical | | |
| **References:** | NIST: [NIST SP 800-53 Revision 4 (v4)](): IA-2 (6) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001938 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |
| **Definition:** | The organization defines the strength of mechanism requirements for the device that is separate from the system gaining access to non-privileged accounts. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IA-2 (7) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001939 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |
| **Definition:** | The information system implements multifactor authentication for network access to non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IA-2 (7) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001940 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |
| **Definition:** | The device used in the information system implementation of multifactor authentication for network access to non-privileged accounts meets organization-defined strength of mechanism requirements. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IA-2 (7) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001941 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |
| **Definition:** | The information system implements replay-resistant authentication mechanisms for network access to privileged accounts. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IA-2 (8) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001942 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |
| **Definition:** | The information system implements replay-resistant authentication mechanisms for network access to non-privileged accounts. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IA-2 (9) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001943 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |
| **Definition:** | The organization defines the information system accounts for which single sign-on capability will be provided. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IA-2 (10) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001944 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |
| **Definition:** | The organization defines the information system services for which single sign-on capability will be provided. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IA-2 (10) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001945 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |
| **Definition:** | The information system provides a single sign-on capability for an organization-defined list of information system accounts. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IA-2 (10) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001946 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |
| **Definition:** | The information system provides a single sign-on capability for an organization-defined list of information system services. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IA-2 (10) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001947 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |
| **Definition:** | The organization defines the strength of mechanism requirements for the device that is separate from the system gaining access and is to provide one factor of a multifactor authentication for remote access to privileged accounts. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IA-2 (11) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001948 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |

**Definition:** The information system implements multifactor authentication for remote access to privileged accounts such that one of the factors is provided by a device separate from the system gaining access.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-2 (11)

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-001949 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |

**Definition:** The device used in the information system implementation of multifactor authentication for remote access to privileged accounts meets organization-defined strength of mechanism requirements.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-2 (11)

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-001950 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |

**Definition:** The organization defines the strength of mechanism requirements for the device that is separate from the system gaining access and is to provide one factor of a multifactor authentication for remote access to non-privileged accounts.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-2 (11)

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-001951 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |

**Definition:** The information system implements multifactor authentication for remote access to non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-2 (11)

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-001952 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |

**Definition:** The device used in the information system implementation of multifactor authentication for remote access to non-privileged accounts meets organization-defined strength of mechanism requirements.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-2 (11)

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-001953 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |

| | | | |
|---|---|---|---|
| **Definition:** | The information system accepts Personal Identity Verification (PIV) credentials. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IA-2 (12) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001954 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |
| **Definition:** | The information system electronically verifies Personal Identity Verification (PIV) credentials. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IA-2 (12) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001955 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |
| **Definition:** | The organization defines the out-of-band authentication to be implemented by the information system under organization-defined conditions. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IA-2 (13) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001956 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |
| **Definition:** | The organization defines the conditions for which the information system implements organization-defined out-of-band authentication. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IA-2 (13) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001957 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |
| **Definition:** | The information system implements organization-defined out-of-band authentication under organization-defined conditions. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IA-2 (13) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000777 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |
| **Definition:** | The organization defines a list of specific and/or types of devices for which identification and authentication is required before establishing a connection to the information system. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): IA-3<br>NIST: NIST SP 800-53 Revision 4 (v4): IA-3 | | |

NIST: NIST SP 800-53A (v1): IA-3.1 (i)

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000778 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |
| **Definition:** | The information system uniquely identifies an organization-defined list of specific and/or types of devices before establishing a local, remote, or network connection. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): IA-3<br>NIST: NIST SP 800-53 Revision 4 (v4): IA-3<br>NIST: NIST SP 800-53A (v1): IA-3.1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001958 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |
| **Definition:** | The information system authenticates an organization-defined list of specific and/or types of devices before establishing a local, remote, or network connection. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IA-3 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001959 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |
| **Definition:** | The organization defines the specific devices and/or type of devices the information system is to authenticate before establishing a connection. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IA-3 (1) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001967 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |
| **Definition:** | The information system authenticates organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection using bidirectional authentication that is cryptographically based. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IA-3 (1) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001960 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |
| **Definition:** | The organization defines the lease information to be assigned to devices. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IA-3 (3) (a) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001961 | **Status:** | draft |

**Contributor:** DISA FSO
**Published Date:** 2013-05-03
**Definition:** The organization defines the lease duration to be assigned to devices.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-3 (3) (a)

---

**CCI:** CCI-001962
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2013-05-03
**Definition:** The organization standardizes dynamic address allocation lease information assigned to devices in accordance with organization-defined lease information.
**Type:** technical
**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-3 (3) (a)

---

**CCI:** CCI-001963
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2013-05-03
**Definition:** The organization standardizes dynamic address allocation lease duration assigned to devices in accordance with organization-defined lease duration.
**Type:** technical
**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-3 (3) (a)

---

**CCI:** CCI-000783
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2009-09-17
**Definition:** The organization audits lease information when assigned to a device.
**Type:** technical
**References:** NIST: NIST SP 800-53 (v3): IA-3 (3)
NIST: NIST SP 800-53 Revision 4 (v4): IA-3 (3) (b)
NIST: NIST SP 800-53A (v1): IA-3 (3).1 (ii)

---

**CCI:** CCI-001964
**Status:** deprecated
**Contributor:** DISA FSO
**Published Date:** 2013-05-03
**Definition:** The organization defines the configuration management process that is to handle the device identification procedures.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-3 (4)

---

**CCI:** CCI-001965
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2013-05-03
**Definition:** The organization defines the configuration management process that is to handle the device authentication procedures.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-3 (4)

---

**CCI:** CCI-001966 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-05-03

**Definition:** The organization ensures that device identification based on attestation is handled by the organization-defined configuration management process.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-3 (4)

---

**CCI:** CCI-001968 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-05-03

**Definition:** The organization defines the configuration management process that is to handle the device identification procedures.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-3 (4)

---

**CCI:** CCI-001969 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-05-03

**Definition:** The organization ensures that device authentication based on attestation is handled by the organization-defined configuration management process.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-3 (4)

---

**CCI:** CCI-001970 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-05-03

**Definition:** The organization defines the personnel or roles that authorize the assignment of individual, group, role, and device identifiers.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-4 a

---

**CCI:** CCI-001971 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-05-03

**Definition:** The organization manages information system identifiers by receiving authorization from organization-defined personnel or roles to assign an individual, group, role, or device identifier.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-4 a

---

**CCI:** CCI-001972 **Status:** draft

| | | | |
|---|---|---|---|
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |
| **Definition:** | The organization manages information system identifiers by selecting an identifier that identifies an individual, group, role, or device. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IA-4 b | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001973 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |
| **Definition:** | The organization manages information system identifiers by assigning the identifier to the intended individual, group, role, or device. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IA-4 c | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001974 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |
| **Definition:** | The organization defines the time period for which the reuse of identifiers is prohibited. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IA-4 d | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001975 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |
| **Definition:** | The organization manages information system identifiers by preventing reuse of identifiers for an organization-defined time period. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IA-4 d | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000794 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |
| **Definition:** | The organization defines a time period of inactivity after which the identifier is disabled. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): IA-4 e<br>NIST: NIST SP 800-53 Revision 4 (v4): IA-4 e<br>NIST: NIST SP 800-53A (v1): IA-4.1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000795 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |
| **Definition:** | The organization manages information system identifiers by disabling the identifier after an organization-defined time period of inactivity. | | |

**Type:** policy, technical

**References:** NIST: NIST SP 800-53 (v3): IA-4 e
NIST: NIST SP 800-53 Revision 4 (v4): IA-4 e
NIST: NIST SP 800-53A (v1): IA-4.1 (iii)

---

**CCI:** CCI-000796 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-17

**Definition:** The organization prohibits the use of information system account identifiers that are the same as public identifiers for individual electronic mail accounts.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): IA-4 (1)
NIST: NIST SP 800-53 Revision 4 (v4): IA-4 (1)
NIST: NIST SP 800-53A (v1): IA-4 (1).1

---

**CCI:** CCI-002040 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-05-03

**Definition:** The organization requires that the registration process to receive an individual identifier includes supervisor authorization.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-4 (2)

---

**CCI:** CCI-000799 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-17

**Definition:** The organization requires multiple forms of certification of individual identification, such as documentary evidence or a combination of documents and biometrics, be presented to the registration authority.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): IA-4 (3)
NIST: NIST SP 800-53 Revision 4 (v4): IA-4 (3)
NIST: NIST SP 800-53A (v1): IA-4 (3).1

---

**CCI:** CCI-000800 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-17

**Definition:** The organization defines characteristics for identifying individual status.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): IA-4 (4)
NIST: NIST SP 800-53 Revision 4 (v4): IA-4 (4)
NIST: NIST SP 800-53A (v1): IA-4 (4).1 (i)

---

**CCI:** CCI-000801 **Status:** draft

**Contributor:** DISA FSO
**Published Date:** 2009-09-17
**Definition:** The organization manages individual identifiers by uniquely identifying each individual by organization-defined characteristics identifying individual status.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): IA-4 (4)
NIST: NIST SP 800-53 Revision 4 (v4): IA-4 (4)
NIST: NIST SP 800-53A (v1): IA-4 (4).1 (ii)

---

**CCI:** CCI-001976
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2013-05-03
**Definition:** The information system dynamically manages identifiers.
**Type:** technical
**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-4 (5)

---

**CCI:** CCI-001977
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2013-05-03
**Definition:** The organization defines the external organizations with which it will coordinate for cross-management of identifiers.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-4 (6)

---

**CCI:** CCI-001978
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2013-05-03
**Definition:** The organization coordinates with organization-defined external organizations for cross-organization management of identifiers.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-4 (6)

---

**CCI:** CCI-001979
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2013-05-03
**Definition:** The organization requires the registration process to receive an individual identifier be conducted in person before a designated registration authority.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-4 (7)

---

**CCI:** CCI-001980
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2013-05-03
**Definition:** The organization manages information system authenticators by verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving

| | | | |
|---|---|---|---|
| | the authenticator. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IA-5 a | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000176 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-05-22 |
| **Definition:** | The organization manages information system authenticators by establishing initial authenticator content for authenticators defined by the organization. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): IA-5 b<br>NIST: NIST SP 800-53 Revision 4 (v4): IA-5 b<br>NIST: NIST SP 800-53A (v1): IA-5.1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001544 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-11-30 |
| **Definition:** | The organization manages information system authenticators by ensuring that authenticators have sufficient strength of mechanism for their intended use. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): IA-5 c<br>NIST: NIST SP 800-53 Revision 4 (v4): IA-5 c<br>NIST: NIST SP 800-53A (v1): IA-5.1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001981 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |
| **Definition:** | The organization manages information system authenticators by establishing administrative procedures for initial authenticator distribution. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IA-5 d | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001982 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |
| **Definition:** | The organization manages information system authenticators by establishing administrative procedures for lost/compromised authenticators. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IA-5 d | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001983 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |
| **Definition:** | The organization manages information system authenticators by establishing administrative | | |

procedures for damaged authenticators.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-5 d

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-001984 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |

**Definition:** The organization manages information system authenticators by establishing administrative procedures for revoking authenticators.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-5 d

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-001985 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |

**Definition:** The organization manages information system authenticators by implementing administrative procedures for initial authenticator distribution.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-5 d

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-001986 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |

**Definition:** The organization manages information system authenticators by implementing administrative procedures for lost/compromised authenticators.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-5 d

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-001987 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |

**Definition:** The organization manages information system authenticators by implementing administrative procedures for damaged authenticators.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-5 d

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-001988 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |

**Definition:** The organization manages information system authenticators by implementing administrative procedures for revoking authenticators.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-5 d

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-001989 | **Status:** | draft |

**Contributor:** DISA FSO **Published Date:** 2013-05-03

**Definition:** The organization manages information system authenticators by changing default content of authenticators prior to information system installation.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-5 e

---

**CCI:** CCI-000179 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-05-22

**Definition:** The organization manages information system authenticators by establishing minimum lifetime restrictions for authenticators.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): IA-5 f

NIST: NIST SP 800-53 Revision 4 (v4): IA-5 f

NIST: NIST SP 800-53A (v1): IA-5.1 (ii)

---

**CCI:** CCI-000180 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-05-22

**Definition:** The organization manages information system authenticators by establishing maximum lifetime restrictions for authenticators.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): IA-5 f

NIST: NIST SP 800-53 Revision 4 (v4): IA-5 f

NIST: NIST SP 800-53A (v1): IA-5.1 (ii)

---

**CCI:** CCI-000181 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-05-22

**Definition:** The organization manages information system authenticators by establishing reuse conditions for authenticators.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): IA-5 f

NIST: NIST SP 800-53 Revision 4 (v4): IA-5 f

NIST: NIST SP 800-53A (v1): IA-5.1 (ii)

---

**CCI:** CCI-001610 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2010-05-12

**Definition:** The organization defines the time period (by authenticator type) for changing/refreshing authenticators.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): IA-5 g

NIST: NIST SP 800-53 Revision 4 (v4): IA-5 g
NIST: NIST SP 800-53A (v1): IA-5.1 (i)

---

**CCI:** CCI-000182 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-05-22
**Definition:** The organization manages information system authenticators by changing/refreshing authenticators in accordance with the organization-defined time period by authenticator type.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): IA-5 g
NIST: NIST SP 800-53 Revision 4 (v4): IA-5 g
NIST: NIST SP 800-53A (v1): IA-5.1 (ii)

---

**CCI:** CCI-000183 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-05-22
**Definition:** The organization manages information system authenticators by protecting authenticator content from unauthorized disclosure.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): IA-5 h
NIST: NIST SP 800-53 Revision 4 (v4): IA-5 h
NIST: NIST SP 800-53A (v1): IA-5.1 (ii)

---

**CCI:** CCI-002042 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-05-03
**Definition:** The organization manages information system authenticators by protecting authenticator content from unauthorized modification.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-5 h

---

**CCI:** CCI-000184 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-05-22
**Definition:** The organization manages information system authenticators by requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): IA-5 i
NIST: NIST SP 800-53 Revision 4 (v4): IA-5 i
NIST: NIST SP 800-53A (v1): IA-5.1 (ii)

---

**CCI:** CCI-002365 **Status:** draft
**Contributor:** DISA FSO **Published** 2013-06-26

**Date:**

**Definition:** The organization manages information system authenticators by requiring individuals to take specific security safeguards to protect authenticators.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-5 i

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002366 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-26 |

**Definition:** The organization manages information system authenticators by having devices implement specific security safeguards to protect authenticators.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-5 i

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001990 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |

**Definition:** The organization manages information system authenticators by changing authenticators for group/role accounts when membership to those accounts changes.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-5 j

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001611 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-12 |

**Definition:** The organization defines the minimum number of special characters for password complexity enforcement.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): IA-5 (1) (a)
NIST: NIST SP 800-53 Revision 4 (v4): IA-5 (1) (a)
NIST: NIST SP 800-53A (v1): IA-5 (1).1 (i)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001612 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-12 |

**Definition:** The organization defines the minimum number of upper case characters for password complexity enforcement.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): IA-5 (1) (a)
NIST: NIST SP 800-53 Revision 4 (v4): IA-5 (1) (a)
NIST: NIST SP 800-53A (v1): IA-5 (1).1 (i)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001613 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published** | 2010-05-12 |

**Date:**

**Definition:** The organization defines the minimum number of lower case characters for password complexity enforcement.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): IA-5 (1) (a)
NIST: NIST SP 800-53 Revision 4 (v4): IA-5 (1) (a)
NIST: NIST SP 800-53A (v1): IA-5 (1).1 (i)

---

**CCI:** CCI-001614 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2010-05-12

**Definition:** The organization defines the minimum number of numeric characters for password complexity enforcement.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): IA-5 (1) (a)
NIST: NIST SP 800-53 Revision 4 (v4): IA-5 (1) (a)
NIST: NIST SP 800-53A (v1): IA-5 (1).1 (i)

---

**CCI:** CCI-001619 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2010-05-12

**Definition:** The information system enforces password complexity by the minimum number of special characters used.

**Type:** technical

**Parameter:** Number of Characters

**References:** NIST: NIST SP 800-53 (v3): IA-5 (1) (a)
NIST: NIST SP 800-53 Revision 4 (v4): IA-5 (1) (a)
NIST: NIST SP 800-53A (v1): IA-5 (1).1 (v)

---

**CCI:** CCI-000192 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-15

**Definition:** The information system enforces password complexity by the minimum number of upper case characters used.

**Type:** technical

**Parameter:** Number of Characters

**References:** NIST: NIST SP 800-53 (v3): IA-5 (1) (a)
NIST: NIST SP 800-53 Revision 4 (v4): IA-5 (1) (a)
NIST: NIST SP 800-53A (v1): IA-5 (1).1 (v)

---

**CCI:** CCI-000193 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-15

**Definition:** The information system enforces password complexity by the minimum number of lower

| | | | |
|---|---|---|---|
| | case characters used. | | |
| **Type:** | technical | | |
| **Parameter:** | Number of Characters | | |
| **References:** | NIST: NIST SP 800-53 (v3): IA-5 (1) (a)<br>NIST: NIST SP 800-53 Revision 4 (v4): IA-5 (1) (a)<br>NIST: NIST SP 800-53A (v1): IA-5 (1).1 (v) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000194 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-15 |
| **Definition:** | The information system enforces password complexity by the minimum number of numeric characters used. | | |
| **Type:** | technical | | |
| **Parameter:** | Number of Characters | | |
| **References:** | NIST: NIST SP 800-53 (v3): IA-5 (1) (a)<br>NIST: NIST SP 800-53 Revision 4 (v4): IA-5 (1) (a)<br>NIST: NIST SP 800-53A (v1): IA-5 (1).1 (v) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000205 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-05-22 |
| **Definition:** | The information system enforces minimum password length. | | |
| **Type:** | technical | | |
| **Parameter:** | Number of Characters | | |
| **References:** | NIST: NIST SP 800-53 (v3): IA-5 (1) (a)<br>NIST: NIST SP 800-53 Revision 4 (v4): IA-5 (1) (a)<br>NIST: NIST SP 800-53A (v1): IA-5 (1).1 (i) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001615 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-12 |
| **Definition:** | The organization defines the minimum number of characters that are changed when new passwords are created. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): IA-5 (1) (b)<br>NIST: NIST SP 800-53 Revision 4 (v4): IA-5 (1) (b)<br>NIST: NIST SP 800-53A (v1): IA-5 (1).1 (ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000195 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-15 |
| **Definition:** | The information system, for password-based authentication, when new passwords are created, enforces that at least an organization-defined number of characters are changed. | | |
| **Type:** | technical | | |

| | | | |
|---|---|---|---|
| **Parameter:** | Number of Characters | | |
| **References:** | NIST: NIST SP 800-53 (v3): IA-5 (1) (b)<br>NIST: NIST SP 800-53 Revision 4 (v4): IA-5 (1) (b)<br>NIST: NIST SP 800-53A (v1): IA-5 (1).1 (v) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000196 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-15 |
| **Definition:** | The information system, for password-based authentication, stores only cryptographically-protected passwords. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): IA-5 (1) (c)<br>NIST: NIST SP 800-53 Revision 4 (v4): IA-5 (1) (c)<br>NIST: NIST SP 800-53A (v1): IA-5 (1).1 (v) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000197 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-15 |
| **Definition:** | The information system, for password-based authentication, transmits only cryptographically-protected passwords. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): IA-5 (1) (c)<br>NIST: NIST SP 800-53 Revision 4 (v4): IA-5 (1) (c)<br>NIST: NIST SP 800-53A (v1): IA-5 (1).1 (v) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001616 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-12 |
| **Definition:** | The organization defines minimum password lifetime restrictions. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): IA-5 (1) (b)<br>NIST: NIST SP 800-53 Revision 4 (v4): IA-5 (1) (d)<br>NIST: NIST SP 800-53A (v1): IA-5 (1).1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001617 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-12 |
| **Definition:** | The organization defines maximum password lifetime restrictions. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): IA-5 (1) (d)<br>NIST: NIST SP 800-53 Revision 4 (v4): IA-5 (1) (d)<br>NIST: NIST SP 800-53A (v1): IA-5 (1).1 (iii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000198 | **Status:** | draft |

**Contributor:** DISA FSO **Published Date:** 2009-09-15

**Definition:** The information system enforces minimum password lifetime restrictions.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): IA-5 (1) (d)
NIST: NIST SP 800-53 Revision 4 (v4): IA-5 (1) (d)
NIST: NIST SP 800-53A (v1): IA-5 (1).1 (v)

---

**CCI:** CCI-000199 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-15

**Definition:** The information system enforces maximum password lifetime restrictions.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): IA-5 (1) (d)
NIST: NIST SP 800-53 Revision 4 (v4): IA-5 (1) (d)
NIST: NIST SP 800-53A (v1): IA-5 (1).1 (v)

---

**CCI:** CCI-001618 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2010-05-12

**Definition:** The organization defines the number of generations for which password reuse is prohibited.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): IA-5 (1) (d)
NIST: NIST SP 800-53 Revision 4 (v4): IA-5 (1) (e)
NIST: NIST SP 800-53A (v1): IA-5 (1).1 (iv)

---

**CCI:** CCI-000200 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-05-22

**Definition:** The information system prohibits password reuse for the organization-defined number of generations.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): IA-5 (1) (e)
NIST: NIST SP 800-53 Revision 4 (v4): IA-5 (1) (e)
NIST: NIST SP 800-53A (v1): IA-5 (1).1 (v)

---

**CCI:** CCI-002041 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-05-03

**Definition:** The information system allows the use of a temporary password for system logons with an immediate change to a permanent password.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-5 (1) (f)

---

**CCI:** CCI-000185 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-15
**Definition:** The information system, for PKI-based authentication, validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information.
**Type:** technical
**References:** NIST: NIST SP 800-53 (v3): IA-5 (2)
NIST: NIST SP 800-53 Revision 4 (v4): IA-5 (2) (a)
NIST: NIST SP 800-53A (v1): IA-5 (2).1

---

**CCI:** CCI-000186 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-15
**Definition:** The information system, for PKI-based authentication, enforces authorized access to the corresponding private key.
**Type:** technical
**References:** NIST: NIST SP 800-53 (v3): IA-5 (2)
NIST: NIST SP 800-53 Revision 4 (v4): IA-5 (2) (b)
NIST: NIST SP 800-53A (v1): IA-5 (2).1

---

**CCI:** CCI-000187 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-15
**Definition:** The information system, for PKI-based authentication, maps the authenticated identity to the account of the individual or group.
**Type:** technical
**References:** NIST: NIST SP 800-53 (v3): IA-5 (2)
NIST: NIST SP 800-53 Revision 4 (v4): IA-5 (2) (c)
NIST: NIST SP 800-53A (v1): IA-5 (2).1

---

**CCI:** CCI-001991 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-05-03
**Definition:** The information system, for PKI-based authentication, implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.
**Type:** technical
**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-5 (2) (d)

---

**CCI:** CCI-001992 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-05-03
**Definition:** The organization defines the personnel or roles responsible for authorizing the organization's registration authority accountable for the authenticator registration process.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-5 (3)

---

**CCI:** CCI-001993 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-05-03

**Definition:** The organization defines the registration authority accountable for the authenticator registration process.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-5 (3)

---

**CCI:** CCI-001994 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-05-03

**Definition:** The organization defines the types of and/or specific authenticators that are subject to the authenticator registration process.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-5 (3)

---

**CCI:** CCI-001995 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-05-03

**Definition:** The organization requires that the registration process, to receive organization-defined types of and/or specific authenticators, be conducted in person, or by a trusted third-party, before an organization-defined registration authority with authorization by organization-defined personnel or roles.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-5 (3)

---

**CCI:** CCI-001996 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-05-03

**Definition:** The organization defines the requirements required by the automated tools to determine if password authenticators are sufficiently strong.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-5 (4)

---

**CCI:** CCI-001997 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-05-03

**Definition:** The organization employs automated tools to determine if password authenticators are sufficiently strong to satisfy organization-defined requirements.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-5 (4)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001998 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |
| **Definition:** | The organization requires developers/installers of information system components to provide unique authenticators or change default authenticators prior to delivery/installation. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IA-5 (5) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000201 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-05-22 |
| **Definition:** | The organization protects authenticators commensurate with the security category of the information to which use of the authenticator permits access. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): IA-5 (6)<br>NIST: NIST SP 800-53 Revision 4 (v4): IA-5 (6)<br>NIST: NIST SP 800-53A (v1): IA-5 (6).1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000202 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-05-22 |
| **Definition:** | The organization ensures unencrypted static authenticators are not embedded in access scripts. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): IA-5 (7)<br>NIST: NIST SP 800-53 Revision 4 (v4): IA-5 (7)<br>NIST: NIST SP 800-53A (v1): IA-5 (7).1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000203 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-05-22 |
| **Definition:** | The organization ensures unencrypted static authenticators are not stored on function keys. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): IA-5 (7)<br>NIST: NIST SP 800-53 Revision 4 (v4): IA-5 (7)<br>NIST: NIST SP 800-53A (v1): IA-5 (7).1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002367 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-06-26 |
| **Definition:** | The organization ensures unencrypted static authenticators are not embedded in applications. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IA-5 (7) | | |

**CCI:** CCI-001621 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2010-05-12
**Definition:** The organization implements organization-defined security safeguards to manage the risk of compromise due to individuals having accounts on multiple information systems.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): IA-5 (8)
NIST: NIST SP 800-53 Revision 4 (v4): IA-5 (8)
NIST: NIST SP 800-53A (v1): IA-5 (8).1 (ii)

---

**CCI:** CCI-000204 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-05-22
**Definition:** The organization defines the security safeguards required to manage the risk of compromise due to individuals having accounts on multiple information systems.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): IA-5 (8)
NIST: NIST SP 800-53 Revision 4 (v4): IA-5 (8)
NIST: NIST SP 800-53A (v1): IA-5 (8).1 (i)

---

**CCI:** CCI-001999 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-05-03
**Definition:** The organization defines the external organizations to be coordinated with for cross-organization management of credentials.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-5 (9)

---

**CCI:** CCI-002000 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-05-03
**Definition:** The organization coordinates with organization-defined external organizations for cross-organization management of credentials.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-5 (9)

---

**CCI:** CCI-002001 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-05-03
**Definition:** The information system dynamically provisions identities.
**Type:** technical
**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-5 (10)

---

**CCI:** CCI-002002 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-05-03

**Definition:** The organization defines the token quality requirements to be employed by the information system mechanisms for token-based authentication.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-5 (11)

---

**CCI:** CCI-002003 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-05-03

**Definition:** The information system, for token-based authentication, employs mechanisms that satisfy organization-defined token quality requirements.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-5 (11)

---

**CCI:** CCI-002004 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-05-03

**Definition:** The organization defines the biometric quality requirements to be employed by the information system mechanisms for biometric-based authentication.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-5 (12)

---

**CCI:** CCI-002005 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-05-03

**Definition:** The information system, for biometric-based authentication, employs mechanisms that satisfy organization-defined biometric quality requirements.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-5 (12)

---

**CCI:** CCI-002006 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-05-03

**Definition:** The organization defines the time period after which the use of cached authenticators is prohibited.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-5 (13)

---

**CCI:** CCI-002007 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-05-03

**Definition:** The information system prohibits the use of cached authenticators after an organization-defined time period.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-5 (13)

---

**CCI:** CCI-002008 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-05-03

**Definition:** The organization, for PKI-based authentication, employs a deliberate organization-wide methodology for managing the content of PKI trust stores installed across all platforms including networks, operating systems, browsers, and applications.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-5 (14)

---

**CCI:** CCI-002043 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-05-03

**Definition:** The organization uses only FICAM-approved path discovery and validation products and services.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-5 (15)

---

**CCI:** CCI-000206 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-05-22

**Definition:** The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

**Type:** technical

**Note:** The feedback from the information system does not provide information that would allow an unauthorized user to compromise the authentication mechanism. Displaying asterisks when a user types in a password is an example of obscuring feedback of authentication information.

**References:** NIST: NIST SP 800-53 (v3): IA-6
NIST: NIST SP 800-53 Revision 4 (v4): IA-6
NIST: NIST SP 800-53A (v1): IA-6.1

---

**CCI:** CCI-000803 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-17

**Definition:** The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): IA-7
NIST: NIST SP 800-53 Revision 4 (v4): IA-7
NIST: NIST SP 800-53A (v1): IA-7.1

---

**CCI:** CCI-000804 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-17

**Definition:** The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): IA-8

NIST: NIST SP 800-53 Revision 4 (v4): IA-8

NIST: NIST SP 800-53A (v1): IA-8.1

---

**CCI:** CCI-002009 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-05-03

**Definition:** The information system accepts Personal Identity Verification (PIV) credentials from other federal agencies.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-8 (1)

---

**CCI:** CCI-002010 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-05-03

**Definition:** The information system electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-8 (1)

---

**CCI:** CCI-002011 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-05-03

**Definition:** The information system accepts FICAM-approved third-party credentials.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-8 (2)

---

**CCI:** CCI-002012 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-05-03

**Definition:** The organization defines the information systems which will employ only FICAM-approved information system components.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-8 (3)

---

**CCI:** CCI-002013 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-05-03

| | | | |
|---|---|---|---|
| **Definition:** | The organization employs only FICAM-approved information system components in organization-defined information systems to accept third-party credentials. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IA-8 (3) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002014 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |
| **Definition:** | The information system conforms to FICAM-issued profiles. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IA-8 (4) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002015 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |
| **Definition:** | The information system accepts Personal Identity Verification-I (PIV-I) credentials. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IA-8 (5) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002016 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |
| **Definition:** | The information system electronically verifies Personal Identity Verification-I (PIV-I) credentials. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IA-8 (5) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002017 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |
| **Definition:** | The organization defines the information system services requiring identification. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IA-9 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002018 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |
| **Definition:** | The organization defines the information system services requiring authentication. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IA-9 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002019 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |

| | |
|---|---|
| **Definition:** | The organization defines the security safeguards to be used when identifying information system services. |
| **Type:** | policy |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IA-9 |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002020 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |
| **Definition:** | The organization defines the security safeguards to be used when authenticating information system services. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IA-9 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002021 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |
| **Definition:** | The organization identifies organization-defined information system services using organization-defined security safeguards. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IA-9 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002022 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |
| **Definition:** | The organization authenticates organization-defined information system services using organization-defined security safeguards. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IA-9 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002023 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |
| **Definition:** | The organization ensures that service providers receive identification information. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IA-9 (1) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002024 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |
| **Definition:** | The organization ensures that service providers validate identification information. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IA-9 (1) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002025 | **Status:** | draft |

**Contributor:** DISA FSO **Published Date:** 2013-05-03

**Definition:** The organization ensures that service providers transmit identification information.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-9 (1)

**CCI:** CCI-002026 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-05-03

**Definition:** The organization ensures that service providers receive authentication information.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-9 (1)

**CCI:** CCI-002027 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-05-03

**Definition:** The organization ensures that service providers validate authentication information.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-9 (1)

**CCI:** CCI-002028 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-05-03

**Definition:** The organization ensures that service providers transmit authentication information.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-9 (1)

**CCI:** CCI-002029 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-05-03

**Definition:** The organization defines the services between which identification decisions are to be transmitted.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-9 (2)

**CCI:** CCI-002030 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-05-03

**Definition:** The organization defines the services between which authentication decisions are to be transmitted.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-9 (2)

**CCI:** CCI-002031 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-05-03

**Definition:** The organization ensures that identification decisions are transmitted between organization-defined services consistent with organizational policies.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-9 (2)

---

**CCI:** CCI-002032 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-05-03

**Definition:** The organization ensures that authentication decisions are transmitted between organization-defined services consistent with organizational policies.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-9 (2)

---

**CCI:** CCI-002033 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-05-03

**Definition:** The organization defines the specific circumstances or situations when individuals accessing an information system employ organization-defined supplemental authentication techniques or mechanisms.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-10

---

**CCI:** CCI-002034 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-05-03

**Definition:** The organization defines the supplemental authentication techniques or mechanisms to be employed in specific organization-defined circumstances or situations by individuals accessing the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-10

---

**CCI:** CCI-002035 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-05-03

**Definition:** The organization requires that individuals accessing the information system employ organization-defined supplemental authentication techniques or mechanisms under specific organization-defined circumstances or situations.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IA-10

---

**CCI:** CCI-002036 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-05-03

| | | | |
|---|---|---|---|
| **Definition:** | The organization defines the circumstances or situations under which users will be required to reauthenticate. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IA-11 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002037 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |
| **Definition:** | The organization defines the circumstances or situations under which devices will be required to reauthenticate. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IA-11 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002038 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |
| **Definition:** | The organization requires users to reauthenticate upon organization-defined circumstances or situations requiring reauthentication. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IA-11 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002039 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-05-03 |
| **Definition:** | The organization requires devices to reauthenticate upon organization-defined circumstances or situations requiring reauthentication. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IA-11 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003519 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-08 |
| **Definition:** | The organization provides means, where feasible and appropriate, for individuals to authorize the collection of personally identifiable information (PII) prior to its collection. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IP-1 a | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003520 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-08 |
| **Definition:** | The organization provides means, where feasible and appropriate, for individuals to authorize the use of personally identifiable information (PII) prior to its collection. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IP-1 a | | |

**CCI:** CCI-003521
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2013-11-08
**Definition:** The organization provides means, where feasible and appropriate, for individuals to authorize the maintaining of personally identifiable information (PII) prior to its collection.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): IP-1 a

---

**CCI:** CCI-003522
**Status:** draft
**Contributor:**
**Published Date:** 2013-11-08
**Definition:** The organization provides means, where feasible and appropriate, for individuals to authorize sharing of personally identifiable information (PII) prior to its collection.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): IP-1 a

---

**CCI:** CCI-003523
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2013-11-08
**Definition:** The organization provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection of personally identifiable information (PII).
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): IP-1 b

---

**CCI:** CCI-003524
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2013-11-08
**Definition:** The organization provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the use of personally identifiable information (PII).
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): IP-1 b

---

**CCI:** CCI-003525
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2013-11-08
**Definition:** The organization provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the dissemination of personally identifiable information (PII).
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): IP-1 b

---

**CCI:** CCI-003526
**Status:** draft
**Contributor:** DISA FSO
**Published** 2013-11-08

**Date:**

**Definition:** The organization provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the retention of personally identifiable information (PII).

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IP-1 b

---

**CCI:** CCI-003527 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-08

**Definition:** The organization obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected personally identifiable information (PII).

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IP-1 c

---

**CCI:** CCI-003528 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-08

**Definition:** The organization ensures that individuals are aware of all uses of personally identifiable information (PII) not initially described in the public notice that was in effect at the time the organization collected the PII.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IP-1 d

---

**CCI:** CCI-003529 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-08

**Definition:** The organization ensures that individuals, where feasible, consent to all uses of personally identifiable information (PII) not initially described in the public notice that was in effect at the time the organization collected the PII.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IP-1 d

---

**CCI:** CCI-003530 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-08

**Definition:** The organization implements mechanisms to support itemized or tiered consent for specific uses of personally identifiable information (PII) data.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IP-1 (1)

---

**CCI:** CCI-003531 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-08

**Definition:** The organization provides individuals the ability to have access to their personally identifiable information (PII) maintained in its system(s) of records.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IP-2 a

---

**CCI:** CCI-003532 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-08

**Definition:** The organization publishes rules governing how individuals may request access to records maintained in a Privacy Act system of records.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IP-2 b

---

**CCI:** CCI-003533 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-08

**Definition:** The organization publishes regulations governing how individuals may request access to records maintained in a Privacy Act system of records.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IP-2 b

---

**CCI:** CCI-003534 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-08

**Definition:** The organization publishes access procedures for Privacy Act systems of records in System of Records Notices (SORNs).

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IP-2 c

---

**CCI:** CCI-003535 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-08

**Definition:** The organization adheres to Privacy Act requirements for the proper processing of Privacy Act requests.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IP-2 d

---

**CCI:** CCI-003536 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-08

**Definition:** The organization adheres to OMB policies and guidance for the proper processing of Privacy Act requests.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IP-2 d

---

**CCI:** CCI-003537 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-08

**Definition:** The organization provides a process for individuals to have inaccurate personally identifiable information (PII) maintained by the organization corrected or amended, as appropriate.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IP-3 a

---

**CCI:** CCI-003538 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-08

**Definition:** The organization establishes a process for disseminating corrections or amendments of the personally identifiable information (PII) to other authorized users of the PII, such as external information-sharing partners.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IP-3 b

---

**CCI:** CCI-003539 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-08

**Definition:** The organization establishes a process, where feasible and appropriate, to notify affected individuals that their personally identifiable information (PII) information has been corrected or amended.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IP-3 b

---

**CCI:** CCI-003540 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-08

**Definition:** The organization implements a process for receiving complaints, concerns, or questions from individuals about the organizational privacy practices.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IP-4

---

**CCI:** CCI-003541 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-08

**Definition:** The organization implements a process for responding to complaints, concerns, or questions from individuals about the organizational privacy practices.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IP-4

---

**CCI:** CCI-003542 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-08

**Definition:** The organization defines the time period within which it must respond to complaints, concerns, or questions from individuals about the organizational privacy practices.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IP-4 (1)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003543 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-08 |

**Definition:** The organization responds to complaints, concerns, or questions from individuals about the organizational privacy practices within the organization-defined time period.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IP-4 (1)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000805 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |

**Definition:** The organization develops and documents an incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): IR-1 a
NIST: NIST SP 800-53 Revision 4 (v4): IR-1 a 1
NIST: NIST SP 800-53A (v1): IR-1.1 (i) (ii)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000806 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |

**Definition:** The organization disseminates an incident response policy to organization-defined personnel or roles.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): IR-1 a
NIST: NIST SP 800-53 Revision 4 (v4): IR-1 a 1
NIST: NIST SP 800-53A (v1): IR-1.1 (iii)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000809 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |

**Definition:** The organization develops and documents procedures to facilitate the implementation of the incident response policy and associated incident response controls.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): IR-1 b
NIST: NIST SP 800-53 Revision 4 (v4): IR-1 a 2
NIST: NIST SP 800-53A (v1): IR-1.1 (iv) (v)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000810 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |

**Definition:** The organization disseminates incident response procedures to organization-defined personnel or roles.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): IR-1 b
NIST: NIST SP 800-53 Revision 4 (v4): IR-1 a 2
NIST: NIST SP 800-53A (v1): IR-1.1 (vi)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002776 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-12 |

**Definition:** The organization defines the personnel or roles to whom the incident response policy is disseminated.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IR-1 a 1

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002777 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-12 |

**Definition:** The organization defines the personnel or roles to whom the incident response procedures are disseminated.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IR-1 a 2

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000807 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |

**Definition:** The organization reviews and updates the current incident response policy in accordance with organization-defined frequency.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): IR-1 a
NIST: NIST SP 800-53 Revision 4 (v4): IR-1 b 1
NIST: NIST SP 800-53A (v1): IR-1.2 (ii)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000808 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |

**Definition:** The organization defines the frequency with which to review and update the current incident response policy.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): IR-1 a
NIST: NIST SP 800-53 Revision 4 (v4): IR-1 b 1

NIST: NIST SP 800-53A (v1): IR-1.2 (i)

---

**CCI:** CCI-000811 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-17

**Definition:** The organization reviews and updates the current incident response procedures in accordance with organization-defined frequency.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): IR-1 b

NIST: NIST SP 800-53 Revision 4 (v4): IR-1 b 2

NIST: NIST SP 800-53A (v1): IR-1.2 (iv)

---

**CCI:** CCI-000812 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-17

**Definition:** The organization defines the frequency with which to review and update the current incident response procedures.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): IR-1 b

NIST: NIST SP 800-53 Revision 4 (v4): IR-1 b 2

NIST: NIST SP 800-53A (v1): IR-1.2 (iii)

---

**CCI:** CCI-000813 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-17

**Definition:** The organization provides incident response training to information system users consistent with assigned roles and responsibilities within an organization-defined time period of assuming an incident response role or responsibility.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): IR-2 a

NIST: NIST SP 800-53 Revision 4 (v4): IR-2 a

NIST: NIST SP 800-53A (v1): IR-2.1 (ii)

---

**CCI:** CCI-002778 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-12

**Definition:** The organization defines the time period in which information system users who assume an incident response role or responsibility receive incident response training.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IR-2 a

---

**CCI:** CCI-002779 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-12

**Definition:** The organization provides incident response training to information system users consistent with assigned roles and responsibilities when required by information system changes.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IR-2 b

---

**CCI:** CCI-000814 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-17

**Definition:** The organization provides incident response training in accordance with organization-defined frequency.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): IR-2 b
NIST: NIST SP 800-53 Revision 4 (v4): IR-2 c
NIST: NIST SP 800-53A (v1): IR-2.1 (v)

---

**CCI:** CCI-000815 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-17

**Definition:** The organization defines a frequency for incident response training.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): IR-2 b
NIST: NIST SP 800-53 Revision 4 (v4): IR-2 c
NIST: NIST SP 800-53A (v1): IR-2.1 (iv)

---

**CCI:** CCI-000816 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-17

**Definition:** The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): IR-2 (1)
NIST: NIST SP 800-53 Revision 4 (v4): IR-2 (1)
NIST: NIST SP 800-53A (v1): IR-2 (1).1

---

**CCI:** CCI-000817 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-17

**Definition:** The organization employs automated mechanisms to provide a more thorough and realistic incident response training environment.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): IR-2 (2)
NIST: NIST SP 800-53 Revision 4 (v4): IR-2 (2)
NIST: NIST SP 800-53A (v1): IR-2 (2).1

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001624 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-12 |
| **Definition:** | The organization documents the results of incident response tests. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): IR-3 | | |
| | NIST: NIST SP 800-53 Revision 4 (v4): IR-3 | | |
| | NIST: NIST SP 800-53A (v1): IR-3.1 (iv) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000818 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |
| **Definition:** | The organization tests the incident response capability for the information system on an organization-defined frequency using organization-defined tests to determine the incident response effectiveness. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): IR-3 | | |
| | NIST: NIST SP 800-53 Revision 4 (v4): IR-3 | | |
| | NIST: NIST SP 800-53A (v1): IR-3.1 (iii) (v) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000819 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |
| **Definition:** | The organization defines a frequency for incident response tests. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): IR-3 | | |
| | NIST: NIST SP 800-53 Revision 4 (v4): IR-3 | | |
| | NIST: NIST SP 800-53A (v1): IR-3.1 (ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000820 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |
| **Definition:** | The organization defines tests for incident response. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): IR-3 | | |
| | NIST: NIST SP 800-53 Revision 4 (v4): IR-3 | | |
| | NIST: NIST SP 800-53A (v1): IR-3.1 (i) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000821 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |
| **Definition:** | The organization employs automated mechanisms to more thoroughly and effectively test the incident response capability. | | |
| **Type:** | policy | | |

| | | | |
|---|---|---|---|
| **References:** | NIST: NIST SP 800-53 (v3): IR-3 (1)<br>NIST: NIST SP 800-53 Revision 4 (v4): IR-3 (1)<br>NIST: NIST SP 800-53A (v1): IR-3 (1).1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002780 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-12 |
| **Definition:** | The organization coordinates incident response testing with organizational elements responsible for related plans. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IR-3 (2) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000822 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |
| **Definition:** | The organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): IR-4 a<br>NIST: NIST SP 800-53 Revision 4 (v4): IR-4 a<br>NIST: NIST SP 800-53A (v1): IR-4.1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000823 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |
| **Definition:** | The organization coordinates incident handling activities with contingency planning activities. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): IR-4 b<br>NIST: NIST SP 800-53 Revision 4 (v4): IR-4 b<br>NIST: NIST SP 800-53A (v1): IR-4.1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001625 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-12 |
| **Definition:** | The organization implements the resulting incident handling activity changes to incident response procedures, training, and testing/exercises accordingly. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): IR-4 c<br>NIST: NIST SP 800-53 Revision 4 (v4): IR-4 c<br>NIST: NIST SP 800-53A (v1): IR-4.1 (iv) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000824 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published** | 2009-09-18 |

| | | | |
|---|---|---|---|
| | | Date: | |
| Definition: | The organization incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises. | | |
| Type: | policy | | |
| References: | NIST: NIST SP 800-53 (v3): IR-4 c<br>NIST: NIST SP 800-53 Revision 4 (v4): IR-4 c<br>NIST: NIST SP 800-53A (v1): IR-4.1 (iii) | | |

| | | | |
|---|---|---|---|
| CCI: | CCI-000825 | Status: | draft |
| Contributor: | DISA FSO | Published Date: | 2009-09-18 |
| Definition: | The organization employs automated mechanisms to support the incident handling process. | | |
| Type: | policy | | |
| References: | NIST: NIST SP 800-53 (v3): IR-4 (1)<br>NIST: NIST SP 800-53 Revision 4 (v4): IR-4 (1)<br>NIST: NIST SP 800-53A (v1): IR-4 (1).1 | | |

| | | | |
|---|---|---|---|
| CCI: | CCI-000826 | Status: | draft |
| Contributor: | DISA FSO | Published Date: | 2009-09-18 |
| Definition: | The organization includes dynamic reconfiguration of organization-defined information system components as part of the incident response capability. | | |
| Type: | policy | | |
| References: | NIST: NIST SP 800-53 (v3): IR-4 (2)<br>NIST: NIST SP 800-53 Revision 4 (v4): IR-4 (2)<br>NIST: NIST SP 800-53A (v1): IR-4 (2).1 | | |

| | | | |
|---|---|---|---|
| CCI: | CCI-002781 | Status: | draft |
| Contributor: | DISA FSO | Published Date: | 2013-07-12 |
| Definition: | The organization defines the information system components for dynamic reconfiguration as part of the incident response capability. | | |
| Type: | policy | | |
| References: | NIST: NIST SP 800-53 Revision 4 (v4): IR-4 (2) | | |

| | | | |
|---|---|---|---|
| CCI: | CCI-000827 | Status: | draft |
| Contributor: | DISA FSO | Published Date: | 2009-09-18 |
| Definition: | The organization defines and identifies classes of incidents for which organization-defined actions are to be taken to ensure continuation of organizational mission and business functions. | | |
| Type: | policy | | |
| References: | NIST: NIST SP 800-53 (v3): IR-4 (3)<br>NIST: NIST SP 800-53 Revision 4 (v4): IR-4 (3) | | |

NIST: NIST SP 800-53A (v1): IR-4 (3).1 (i)

---

**CCI:** CCI-000828 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization defines and identifies actions to take in response to organization-defined classes of incidents to ensure continuation of organizational missions and business functions.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): IR-4 (3)

NIST: NIST SP 800-53 Revision 4 (v4): IR-4 (3)

NIST: NIST SP 800-53A (v1): IR-4 (3).1 (ii)

---

**CCI:** CCI-000829 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): IR-4 (4)

NIST: NIST SP 800-53 Revision 4 (v4): IR-4 (4)

NIST: NIST SP 800-53A (v1): IR-4 (4).1

---

**CCI:** CCI-000830 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization defines security violations that, if detected, initiate a configurable capability to automatically disable the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): IR-4 (5)

NIST: NIST SP 800-53 Revision 4 (v4): IR-4 (5)

NIST: NIST SP 800-53A (v1): IR-4 (5).1 (i)

---

**CCI:** CCI-000831 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization implements a configurable capability to automatically disable the information system if organization-defined security violations are detected.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): IR-4 (5)

NIST: NIST SP 800-53 Revision 4 (v4): IR-4 (5)

NIST: NIST SP 800-53A (v1): IR-4 (5).1 (ii)

---

**CCI:** CCI-002782 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-12

**Definition:** The organization implements an incident handling capability for insider threats.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IR-4 (6)

---

**CCI:** CCI-002783 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-12

**Definition:** The organization coordinates an incident handling capability for insider threats across organization-defined components or elements of the organization.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IR-4 (7)

---

**CCI:** CCI-002784 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-12

**Definition:** The organization defines components or elements of the organization across which an incident handling capability for insider threats will be coordinated.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IR-4 (7)

---

**CCI:** CCI-002785 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-12

**Definition:** The organization coordinates with organization-defined external organizations to correlate and share organization-defined incident information to achieve a cross-organization perspective on incident awareness and more effective incident responses.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IR-4 (8)

---

**CCI:** CCI-002786 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-12

**Definition:** The organization defines external organizations with which to correlate and share organization-defined incident information.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IR-4 (8)

---

**CCI:** CCI-002787 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-12

**Definition:** The organization defines incident information to correlate and share with organization-defined external organizations.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IR-4 (8)

---

**CCI:** CCI-002788 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-12

**Definition:** The organization employs organization-defined dynamic response capabilities to effectively respond to security incidents.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IR-4 (9)

---

**CCI:** CCI-002789 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-12

**Definition:** The organization defines dynamic response capabilities to effectively respond to security incidents.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IR-4 (9)

---

**CCI:** CCI-002790 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-12

**Definition:** The organization coordinates incident handling activities involving supply chain events with other organizations involved in the supply chain.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IR-4 (10)

---

**CCI:** CCI-000832 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization tracks and documents information system security incidents.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): IR-5
NIST: NIST SP 800-53 Revision 4 (v4): IR-5
NIST: NIST SP 800-53A (v1): IR-5.1

---

**CCI:** CCI-001626 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2010-05-12

**Definition:** The organization employs automated mechanisms to assist in the collection of security incident information.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): IR-5 (1)
NIST: NIST SP 800-53 Revision 4 (v4): IR-5 (1)
NIST: NIST SP 800-53A (v1): IR-5 (1).1 (ii)

---

**CCI:** CCI-001627 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2010-05-12

**Definition:** The organization employs automated mechanisms to assist in the analysis of security incident information.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): IR-5 (1)

NIST: NIST SP 800-53 Revision 4 (v4): IR-5 (1)

NIST: NIST SP 800-53A (v1): IR-5 (1).1 (iii)

---

**CCI:** CCI-000833 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization employs automated mechanisms to assist in the tracking of security incidents.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): IR-5 (1)

NIST: NIST SP 800-53 Revision 4 (v4): IR-5 (1)

NIST: NIST SP 800-53A (v1): IR-5 (1).1 (i)

---

**CCI:** CCI-000834 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization defines a time period for personnel to report suspected security incidents to the organizational incident response capability.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): IR-6 a

NIST: NIST SP 800-53 Revision 4 (v4): IR-6 a

NIST: NIST SP 800-53A (v1): IR-6.1 (i)

---

**CCI:** CCI-000835 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization requires personnel to report suspected security incidents to the organizational incident response capability within the organization-defined time period.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): IR-6 a

NIST: NIST SP 800-53 Revision 4 (v4): IR-6 a

NIST: NIST SP 800-53A (v1): IR-6.1 (ii)

---

**CCI:** CCI-000836 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization reports security incident information to organization-defined authorities.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): IR-6 b
NIST: NIST SP 800-53 Revision 4 (v4): IR-6 b
NIST: NIST SP 800-53A (v1): IR-6.1 (iii)

---

**CCI:** CCI-002791 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-07-12

**Definition:** The organization defines authorities to whom security incident information is reported.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IR-6 b

---

**CCI:** CCI-000837 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization employs automated mechanisms to assist in the reporting of security incidents.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): IR-6 (1)
NIST: NIST SP 800-53 Revision 4 (v4): IR-6 (1)
NIST: NIST SP 800-53A (v1): IR-6 (1).1

---

**CCI:** CCI-000838 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization reports information system vulnerabilities associated with reported security incidents to organization-defined personnel or roles.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): IR-6 (2)
NIST: NIST SP 800-53 Revision 4 (v4): IR-6 (2)
NIST: NIST SP 800-53A (v1): IR-6 (2).1

---

**CCI:** CCI-002792 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-07-12

**Definition:** The organization defines personnel or roles to whom information system vulnerabilities associated with reported security incident information are reported.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IR-6 (2)

---

**CCI:** CCI-002793 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-07-12

**Definition:** The organization provides security incident information to other organizations involved in the supply chain for information systems or information system components related to the incident.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IR-6 (3)

---

**CCI:** CCI-000839 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization provides an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): IR-7
NIST: NIST SP 800-53 Revision 4 (v4): IR-7
NIST: NIST SP 800-53A (v1): IR-7.1 (i) (ii)

---

**CCI:** CCI-000840 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization employs automated mechanisms to increase the availability of incident response-related information and support.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): IR-7 (1)
NIST: NIST SP 800-53 Revision 4 (v4): IR-7 (1)
NIST: NIST SP 800-53A (v1): IR-7 (1).1

---

**CCI:** CCI-000841 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization establishes a direct, cooperative relationship between its incident response capability and external providers of information system protection capability.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): IR-7 (2) (a)
NIST: NIST SP 800-53 Revision 4 (v4): IR-7 (2) (a)
NIST: NIST SP 800-53A (v1): IR-7 (2).1 (i)

---

**CCI:** CCI-000842 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization identifies organizational incident response team members to the external providers.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): IR-7 (2) (b)
NIST: NIST SP 800-53 Revision 4 (v4): IR-7 (2) (b)

NIST: NIST SP 800-53A (v1): IR-7 (2).1 (ii)

---

**CCI:** CCI-000844 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization develops an incident response plan that is reviewed and approved by organization-defined personnel or roles.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): IR-8 a

NIST: NIST SP 800-53 Revision 4 (v4): IR-8 a 8

NIST: NIST SP 800-53A (v1): IR-8.1

---

**CCI:** CCI-002794 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-12

**Definition:** The organization develops an incident response plan.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IR-8 a

---

**CCI:** CCI-002795 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-12

**Definition:** The organization's incident response plan provides the organization with a roadmap for implementing its incident response capability.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IR-8 a 1

---

**CCI:** CCI-002796 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-12

**Definition:** The organization's incident response plan describes the structure and organization of the incident response capability.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IR-8 a 2

---

**CCI:** CCI-002797 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-12

**Definition:** The organization's incident response plan provides a high-level approach for how the incident response capability fits into the overall organization.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IR-8 a 3

---

**CCI:** CCI-002798 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-12

**Definition:** The organization's incident response plan meets the unique requirements of the organization, which relate to mission, size, structure, and functions.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IR-8 a 4

---

**CCI:** CCI-002799 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-12

**Definition:** The organization's incident response plan defines reportable incidents.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IR-8 a 5

---

**CCI:** CCI-002800 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-12

**Definition:** The organization's incident response plan provides metrics for measuring the incident response capability within the organization.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IR-8 a 6

---

**CCI:** CCI-002801 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-12

**Definition:** The organization's incident response plan defines the resources and management support needed to effectively maintain and mature an incident response capability.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IR-8 a 7

---

**CCI:** CCI-002802 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-12

**Definition:** The organization defines personnel or roles to review and approve the incident response plan.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IR-8 a 8

---

**CCI:** CCI-000845 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization defines incident response personnel (identified by name and/or by role) and organizational elements to whom copies of the incident response plan are distributed.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): IR-8 b

NIST: NIST SP 800-53 Revision 4 (v4): IR-8 b
NIST: NIST SP 800-53A (v1): IR-8.2 (i)

---

**CCI:** CCI-000846 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-18
**Definition:** The organization distributes copies of the incident response plan to organization-defined incident response personnel (identified by name and/or by role) and organizational elements.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): IR-8 b
NIST: NIST SP 800-53 Revision 4 (v4): IR-8 b
NIST: NIST SP 800-53A (v1): IR-8.2 (ii)

---

**CCI:** CCI-000847 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-18
**Definition:** The organization defines the frequency for reviewing the incident response plan.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): IR-8 c
NIST: NIST SP 800-53 Revision 4 (v4): IR-8 c
NIST: NIST SP 800-53A (v1): IR-8.2 (iii)

---

**CCI:** CCI-000848 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-18
**Definition:** The organization reviews the incident response plan on an organization-defined frequency.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): IR-8 c
NIST: NIST SP 800-53 Revision 4 (v4): IR-8 c
NIST: NIST SP 800-53A (v1): IR-8.2 (iv)

---

**CCI:** CCI-000849 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-18
**Definition:** The organization updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): IR-8 d
NIST: NIST SP 800-53 Revision 4 (v4): IR-8 d
NIST: NIST SP 800-53A (v1): IR-8.2 (v)

---

**CCI:** CCI-000850 **Status:** draft
**Contributor:** DISA FSO **Published** 2009-09-18

**Date:**

**Definition:** The organization communicates incident response plan changes to organization-defined incident response personnel (identified by name and/or by role) and organizational elements.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): IR-8 e

NIST: NIST SP 800-53 Revision 4 (v4): IR-8 e

NIST: NIST SP 800-53A (v1): IR-8.2 (vi)

---

**CCI:** CCI-002803 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-12

**Definition:** The organization defines incident response personnel (identified by name and/or by role) and organizational elements to whom incident response plan changes will be communicated.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IR-8 e

---

**CCI:** CCI-002804 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-12

**Definition:** The organization protects the incident response plan from unauthorized disclosure and modification.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IR-8 f

---

**CCI:** CCI-002805 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-12

**Definition:** The organization responds to information spills by identifying the specific information involved in the information system contamination.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IR-9 a

---

**CCI:** CCI-002806 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-12

**Definition:** The organization responds to information spills by alerting organization-defined personnel or roles of the information spill using a method of communication not associated with the spill.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IR-9 b

---

**CCI:** CCI-002807 **Status:** draft

**Contributor:** DISA FSO **Published** 2013-07-12

**Date:**

**Definition:** The organization defines personnel or roles to be alerted of information spills using a method of communication not associated with the spill.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IR-9 b

---

**CCI:** CCI-002808 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-12

**Definition:** The organization responds to information spills by isolating the contaminated information system or system component.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IR-9 c

---

**CCI:** CCI-002809 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-12

**Definition:** The organization responds to information spills by eradicating the information from the contaminated information system or component.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IR-9 d

---

**CCI:** CCI-002810 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-12

**Definition:** The organization responds to information spills by identifying other information systems or system components that may have been subsequently contaminated.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IR-9 e

---

**CCI:** CCI-002811 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-12

**Definition:** The organization responds to information spills by performing other organization-defined actions.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IR-9 f

---

**CCI:** CCI-002812 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-12

**Definition:** The organization defines other actions required to respond to information spills.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IR-9 f

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-002813 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-12 |
| **Definition:** | The organization assigns organization-defined personnel or roles with responsibility for responding to information spills. |  |  |
| **Type:** | policy |  |  |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IR-9 (1) |  |  |

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-002814 | **Status:** | deprecated |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-12 |
| **Definition:** | The organization assigns organization-defined personnel or roles with responsibility for responding to information spills. |  |  |
| **Type:** | policy |  |  |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IR-9 (1) |  |  |

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-002815 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-12 |
| **Definition:** | The organization defines personnel or roles to whom responsibility for responding to information spills will be assigned. |  |  |
| **Type:** | policy |  |  |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IR-9 (1) |  |  |

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-002816 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-12 |
| **Definition:** | The organization provides information spillage response training according to an organization-defined frequency. |  |  |
| **Type:** | policy |  |  |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IR-9 (2) |  |  |

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-002817 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-12 |
| **Definition:** | The organization defines the frequency with which to provide information spillage response training. |  |  |
| **Type:** | policy |  |  |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): IR-9 (2) |  |  |

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-002818 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-12 |
| **Definition:** | The organization implements organization-defined procedures to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while |  |  |

contaminated systems are undergoing corrective actions.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IR-9 (3)

---

**CCI:** CCI-002819 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-12

**Definition:** The organization defines procedures to implement to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IR-9 (3)

---

**CCI:** CCI-002820 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-12

**Definition:** The organization employs organization-defined security safeguards for personnel exposed to information not within assigned access authorizations.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IR-9 (4)

---

**CCI:** CCI-002821 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-12

**Definition:** The organization defines security safeguards to employ for personnel exposed to information not within assigned access authorizations.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IR-9 (4)

---

**CCI:** CCI-002822 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-12

**Definition:** The organization establishes an integrated team of forensic/malicious code analysts, tool developers, and real-time operations personnel.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): IR-10

---

**CCI:** CCI-000855 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization develops and documents procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): MA-1 b
NIST: NIST SP 800-53 Revision 4 (v4): MA-1 a 2

| | | | |
|---|---|---|---|
| | NIST: NIST SP 800-53A (v1): MA-1.1 (iv and v) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000856 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |
| **Definition:** | The organization disseminates to organization-defined personnel or roles procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): MA-1 b<br>NIST: NIST SP 800-53 Revision 4 (v4): MA-1 a 2<br>NIST: NIST SP 800-53A (v1): MA-1.1 (vi) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000852 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |
| **Definition:** | The organization develops and documents a system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): MA-1 a<br>NIST: NIST SP 800-53 Revision 4 (v4): MA-1 a 1<br>NIST: NIST SP 800-53A (v1): MA-1.1 (i and ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000853 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |
| **Definition:** | The organization disseminates to organization-defined personnel or roles a system maintenance policy. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): MA-1 a<br>NIST: NIST SP 800-53 Revision 4 (v4): MA-1 a 1<br>NIST: NIST SP 800-53A (v1): MA-1.1 (iii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002861 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-22 |
| **Definition:** | The organization defines the personnel or roles to whom a system maintenance policy is disseminated. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): MA-1 a 1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002862 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-22 |

**Definition:** The organization defines the personnel or roles to whom system maintenance procedures are to be disseminated.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): MA-1 a 2

---

**CCI:** CCI-001628 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2010-05-12

**Definition:** The organization defines a frequency with which to review and update the current system maintenance procedures.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): MA-1
NIST: NIST SP 800-53 Revision 4 (v4): MA-1 b 2
NIST: NIST SP 800-53A (v1): MA-1.2 (iii)

---

**CCI:** CCI-000854 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization reviews and updates the current system maintenance policy in accordance with organization-defined frequency.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): MA-1 a
NIST: NIST SP 800-53 Revision 4 (v4): MA-1 b 1
NIST: NIST SP 800-53A (v1): MA-1.2 (ii)

---

**CCI:** CCI-000857 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization reviews and updates the current system maintenance procedures in accordance with organization-defined frequency.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): MA-1 b
NIST: NIST SP 800-53 Revision 4 (v4): MA-1 b 2
NIST: NIST SP 800-53A (v1): MA-1.2 (iv)

---

**CCI:** CCI-000851 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization defines the frequency with which to review and update the current system maintenance policy.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): MA-1
NIST: NIST SP 800-53 Revision 4 (v4): MA-1 b 1
NIST: NIST SP 800-53A (v1): MA-1.2 (i)

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002866 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-22 |
| **Definition:** | The organization schedules maintenance on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): MA-2 a | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002867 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-22 |
| **Definition:** | The organization performs maintenance on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): MA-2 a | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002868 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-22 |
| **Definition:** | The organization documents maintenance on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): MA-2 a | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002869 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-22 |
| **Definition:** | The organization reviews records of maintenance on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): MA-2 a | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002870 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-22 |
| **Definition:** | The organization schedules repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): MA-2 a | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002871 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-22 |
| **Definition:** | The organization performs repairs on information system components in accordance with | | |

manufacturer or vendor specifications and/or organizational requirements.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): MA-2 a

---

**CCI:** CCI-002872 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-22

**Definition:** The organization documents repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): MA-2 a

---

**CCI:** CCI-002873 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-22

**Definition:** The organization reviews records of repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): MA-2 a

---

**CCI:** CCI-000859 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): MA-2 b
NIST: NIST SP 800-53 Revision 4 (v4): MA-2 b
NIST: NIST SP 800-53A (v1): MA-2.1 (ii)

---

**CCI:** CCI-000860 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization requires that organization-defined personnel or roles explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): MA-2 c
NIST: NIST SP 800-53 Revision 4 (v4): MA-2 c
NIST: NIST SP 800-53A (v1): MA-2.1 (iii)

---

**CCI:** CCI-002874 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-22

**Definition:** The organization defines the personnel or roles who can explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): MA-2 c

---

**CCI:** CCI-000861 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): MA-2 d
NIST: NIST SP 800-53 Revision 4 (v4): MA-2 d
NIST: NIST SP 800-53A (v1): MA-2.1 (iv)

---

**CCI:** CCI-000862 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): MA-2 e
NIST: NIST SP 800-53 Revision 4 (v4): MA-2 e
NIST: NIST SP 800-53A (v1): MA-2.1 (v)

---

**CCI:** CCI-002875 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-22

**Definition:** The organization includes organization-defined maintenance-related information in organizational maintenance records.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): MA-2 f

---

**CCI:** CCI-002876 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-22

**Definition:** The organization defines the maintenance-related information to include in organizational maintenance records.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): MA-2 f

---

**CCI:** CCI-002863 **Status:** draft

**Contributor:** DISA FSO **Published** 2013-07-22

| | | | |
|---|---|---|---|
| | | **Date:** | |
| **Definition:** | The organization employs automated mechanisms to schedule, conduct, and document repairs. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): MA-2 (2) (a) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002905 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-08-12 |
| **Definition:** | The organization employs automated mechanisms to schedule, conduct, and document maintenance. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): MA-2 (2) (a) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002864 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-22 |
| **Definition:** | The organization produces up-to date, accurate, and complete records of all maintenance requested, scheduled, in process, and completed. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): MA-2 (2) (b) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002865 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-22 |
| **Definition:** | The organization produces up-to date, accurate, and complete records of all repair actions requested, scheduled, in process, and completed. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): MA-2 (2) (b) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000865 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |
| **Definition:** | The organization approves information system maintenance tools. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): MA-3<br>NIST: NIST SP 800-53 Revision 4 (v4): MA-3<br>NIST: NIST SP 800-53A (v1): MA-3.1 (i) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000866 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |
| **Definition:** | The organization controls information system maintenance tools. | | |
| **Type:** | policy | | |

**References:** NIST: NIST SP 800-53 (v3): MA-3
NIST: NIST SP 800-53 Revision 4 (v4): MA-3
NIST: NIST SP 800-53A (v1): MA-3.1 (i)

---

**CCI:** CCI-000867 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-18
**Definition:** The organization monitors information system maintenance tools.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): MA-3
NIST: NIST SP 800-53 Revision 4 (v4): MA-3
NIST: NIST SP 800-53A (v1): MA-3.1 (i)

---

**CCI:** CCI-000869 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-18
**Definition:** The organization inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): MA-3 (1)
NIST: NIST SP 800-53 Revision 4 (v4): MA-3 (1)
NIST: NIST SP 800-53A (v1): MA-3 (1).1

---

**CCI:** CCI-000870 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-18
**Definition:** The organization checks media containing diagnostic and test programs for malicious code before the media are used in the information system.
**Type:** policy, technical
**References:** NIST: NIST SP 800-53 (v3): MA-3 (2)
NIST: NIST SP 800-53 Revision 4 (v4): MA-3 (2)
NIST: NIST SP 800-53A (v1): MA-3 (2).1

---

**CCI:** CCI-000871 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-18
**Definition:** The organization prevents the unauthorized removal of maintenance equipment containing organizational information by: (a) verifying that there is no organizational information contained on the equipment; (b) sanitizing or destroying the equipment; (c) retaining the equipment within the facility; or (d) obtaining an exemption from organization-defined personnel or roles explicitly authorizing removal of the equipment from the facility.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): MA-3 (3)
NIST: NIST SP 800-53 Revision 4 (v4): MA-3 (3)

NIST: NIST SP 800-53A (v1): MA-3 (3).1

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002877 | **Status:** | deprecated |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-22 |
| **Definition:** | The organization prevents the unauthorized removal of maintenance equipment containing organizational information by verifying that there is no organizational information contained on the equipment. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): MA-3 (3) (a) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002878 | **Status:** | deprecated |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-22 |
| **Definition:** | The organization prevents the unauthorized removal of maintenance equipment containing organizational information by sanitizing or destroying the equipment. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): MA-3 (3) (b) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002879 | **Status:** | deprecated |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-22 |
| **Definition:** | The organization prevents the unauthorized removal of maintenance equipment containing organizational information by retaining the equipment within the facility. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): MA-3 (3) (c) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002880 | **Status:** | deprecated |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-22 |
| **Definition:** | The organization prevents the unauthorized removal of maintenance equipment containing organizational information by retaining the equipment within the facility. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): MA-3 (3) (c) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002881 | **Status:** | deprecated |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-22 |
| **Definition:** | The organization prevents the unauthorized removal of maintenance equipment containing organizational information by obtaining an exemption from organization-defined personnel or roles explicitly authorizing removal of the equipment from the facility. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): MA-3 (3) (d) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002882 | **Status:** | draft |

**Contributor:** DISA FSO **Published Date:** 2013-07-22

**Definition:** The organization defines the personnel or roles who can provide an exemption that explicitly authorizes removal of equipment from the facility.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): MA-3 (3) (d)

---

**CCI:** CCI-002883 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-22

**Definition:** The information system restricts the use of maintenance tools to authorized personnel only.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): MA-3 (4)

---

**CCI:** CCI-000873 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization approves nonlocal maintenance and diagnostic activities.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): MA-4 a
NIST: NIST SP 800-53 Revision 4 (v4): MA-4 a
NIST: NIST SP 800-53A (v1): MA-4.1 (i)

---

**CCI:** CCI-000874 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization monitors nonlocal maintenance and diagnostic activities.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): MA-4 a
NIST: NIST SP 800-53 Revision 4 (v4): MA-4 a
NIST: NIST SP 800-53A (v1): MA-4.1 (i)

---

**CCI:** CCI-000876 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): MA-4 b
NIST: NIST SP 800-53 Revision 4 (v4): MA-4 b
NIST: NIST SP 800-53A (v1): MA-4.1 (iii)

---

**CCI:** CCI-000877 **Status:** draft

| | | | |
|---|---|---|---|
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |
| **Definition:** | The organization employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): MA-4 c<br>NIST: NIST SP 800-53 Revision 4 (v4): MA-4 c<br>NIST: NIST SP 800-53A (v1): MA-4.1 (iv) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000878 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |
| **Definition:** | The organization maintains records for nonlocal maintenance and diagnostic activities. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): MA-4 d<br>NIST: NIST SP 800-53 Revision 4 (v4): MA-4 d<br>NIST: NIST SP 800-53A (v1): MA-4.1 (v) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000879 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |
| **Definition:** | The organization terminates sessions and network connections when nonlocal maintenance is completed. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): MA-4 e<br>NIST: NIST SP 800-53 Revision 4 (v4): MA-4 e<br>NIST: NIST SP 800-53A (v1): MA-4.1 (vi) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002884 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-22 |
| **Definition:** | The organization audits nonlocal maintenance and diagnostic sessions' organization-defined audit events. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): MA-4 (1) (a) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002885 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-22 |
| **Definition:** | The organization defines the nonlocal maintenance and diagnostic session audit events to audit. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): MA-4 (1) (a) | | |

**CCI:** CCI-002886 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-07-22
**Definition:** The organization reviews the records of the nonlocal maintenance and diagnostic sessions.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): MA-4 (1) (b)

---

**CCI:** CCI-000881 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-18
**Definition:** The organization documents, in the security plan for the information system, the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): MA-4 (2)
NIST: NIST SP 800-53 Revision 4 (v4): MA-4 (2)
NIST: NIST SP 800-53A (v1): MA-4 (2).1

---

**CCI:** CCI-000882 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-18
**Definition:** The organization requires that nonlocal maintenance and diagnostic services be performed from an information system that implements a security capability comparable to the capability implemented on the system being serviced.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): MA-4 (3) (a)
NIST: NIST SP 800-53 Revision 4 (v4): MA-4 (3) (a)
NIST: NIST SP 800-53A (v1): MA-4 (3).1 (i)

---

**CCI:** CCI-001631 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2010-05-12
**Definition:** The organization, before removal from organizational facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software) before reconnecting the component to the information system.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): MA-4 (3) (b)
NIST: NIST SP 800-53 Revision 4 (v4): MA-4 (3) (b)
NIST: NIST SP 800-53A (v1): MA-4 (3).1 (iii)

---

**CCI:** CCI-000883 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-18
**Definition:** The organization removes the component to be serviced from the information system and prior to nonlocal maintenance or diagnostic services, sanitizes the component (with regard

| | | | |
|---|---|---|---|
| | to organizational information) before removal from organizational facilities. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): MA-4 (3) (b)<br>NIST: NIST SP 800-53 Revision 4 (v4): MA-4 (3) (b)<br>NIST: NIST SP 800-53A (v1): MA-4 (3).1 (i) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000884 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |
| **Definition:** | The organization protects nonlocal maintenance sessions by employing organization-defined authenticators that are replay resistant. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): MA-4 (4)<br>NIST: NIST SP 800-53 Revision 4 (v4): MA-4 (4) (a)<br>NIST: NIST SP 800-53A (v1): MA-4 (4).1 (i) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002887 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-22 |
| **Definition:** | The organization defines the authenticators that are replay resistant which will be employed to protect nonlocal maintenance sessions. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): MA-4 (4) (a) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001632 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-12 |
| **Definition:** | The organization protects nonlocal maintenance sessions by separating the maintenance session from other network sessions with the information system by either physically separated communications paths or logically separated communications paths based upon encryption. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): MA-4 (4) (a) (b)<br>NIST: NIST SP 800-53 Revision 4 (v4): MA-4 (4) (b)<br>NIST: NIST SP 800-53A (v1): MA-4 (4).1 (ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000887 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |
| **Definition:** | The organization requires the approval of each nonlocal maintenance session by organization-defined personnel or roles. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): MA-4 (5) (b)<br>NIST: NIST SP 800-53 Revision 4 (v4): MA-4 (5) (a) | | |

|  |  |  |  |
|---|---|---|---|
|  | NIST: NIST SP 800-53A (v1): MA-4 (5).1 (iii) |  |  |

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-002888 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-22 |
| **Definition:** | The organization defines the personnel or roles authorized to approve each nonlocal maintenance session. |  |  |
| **Type:** | policy |  |  |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): MA-4 (5) (a) |  |  |

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-000886 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |
| **Definition:** | The organization defines the personnel or roles to be notified of the date and time of planned nonlocal maintenance. |  |  |
| **Type:** | policy |  |  |
| **References:** | NIST: NIST SP 800-53 (v3): MA-4 (5) (a)<br>NIST: NIST SP 800-53 Revision 4 (v4): MA-4 (5) (b)<br>NIST: NIST SP 800-53A (v1): MA-4 (5).1 (ii) |  |  |

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-002889 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-22 |
| **Definition:** | The organization notifies organization-defined personnel or roles of the date and time of planned nonlocal maintenance. |  |  |
| **Type:** | policy |  |  |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): MA-4 (5) (b) |  |  |

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-002890 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-22 |
| **Definition:** | The information system implements cryptographic mechanisms to protect the integrity of nonlocal maintenance and diagnostic communications. |  |  |
| **Type:** | technical |  |  |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): MA-4 (6) |  |  |

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-003123 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-24 |
| **Definition:** | The information system implements cryptographic mechanisms to protect the confidentiality of nonlocal maintenance and diagnostic communications. |  |  |
| **Type:** | technical |  |  |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): MA-4 (6) |  |  |

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-002891 | **Status:** | draft |

| | | | |
|---|---|---|---|
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-22 |
| **Definition:** | The information system implements remote disconnect verification at the termination of nonlocal maintenance and diagnostic sessions. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): MA-4 (7) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000890 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |
| **Definition:** | The organization establishes a process for maintenance personnel authorization. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): MA-5 a<br>NIST: NIST SP 800-53 Revision 4 (v4): MA-5 a<br>NIST: NIST SP 800-53A (v1): MA-5.1 (i) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000891 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |
| **Definition:** | The organization maintains a list of authorized maintenance organizations or personnel. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): MA-5 a<br>NIST: NIST SP 800-53 Revision 4 (v4): MA-5 a<br>NIST: NIST SP 800-53A (v1): MA-5.1 (ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002894 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-22 |
| **Definition:** | The organization ensures that non-escorted personnel performing maintenance on the information system have required access authorizations. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): MA-5 b | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002895 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-22 |
| **Definition:** | The organization designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): MA-5 c | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000893 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published** | 2009-09-18 |

| | | | |
|---|---|---|---|
| | | **Date:** | |
| **Definition:** | The organization implements procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): MA-5 (1)<br>NIST: NIST SP 800-53 Revision 4 (v4): MA-5 (1) (a)<br>NIST: NIST SP 800-53A (v1): MA-5 (1).1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000894 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |
| **Definition:** | The organization requires maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals to be escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): MA-5 (1) (a)<br>NIST: NIST SP 800-53 Revision 4 (v4): MA-5 (1) (a) (1)<br>NIST: NIST SP 800-53A (v1): MA-5 (1).1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000895 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |
| **Definition:** | The organization requires that, prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the information system be sanitized and all nonvolatile storage media be removed or physically disconnected from the system and secured. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): MA-5 (1) (b)<br>NIST: NIST SP 800-53 Revision 4 (v4): MA-5 (1) (a) (2)<br>NIST: NIST SP 800-53A (v1): MA-5 (1).1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002892 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-22 |
| **Definition:** | The organization develops and implements alternate security safeguards in the event an information system component cannot be sanitized, removed, or disconnected from the system. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): MA-5 (1) (b) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000897 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published** | 2009-09-18 |

**Date:**

**Definition:** The organization ensures that personnel performing maintenance and diagnostic activities on an information system processing, storing, or transmitting classified information possess security clearances and formal access approvals for at least the highest classification level and for all compartments of information on the system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): MA-5 (2)
NIST: NIST SP 800-53 Revision 4 (v4): MA-5 (2)
NIST: NIST SP 800-53A (v1): MA-5 (2).1

---

**CCI:** CCI-000898 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization ensures that personnel performing maintenance and diagnostic activities on an information system processing, storing, or transmitting classified information are U.S. citizens.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): MA-5 (3)
NIST: NIST SP 800-53 Revision 4 (v4): MA-5 (3)
NIST: NIST SP 800-53A (v1): MA-5 (3).1

---

**CCI:** CCI-000899 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization ensures that cleared foreign nationals (i.e., foreign nationals with appropriate security clearances) are used to conduct maintenance and diagnostic activities on classified information systems only when the systems are jointly owned and operated by the United States and foreign allied governments, or owned and operated solely by foreign allied governments.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): MA-5 (4) (a)
NIST: NIST SP 800-53 Revision 4 (v4): MA-5 (4) (a)
NIST: NIST SP 800-53A (v1): MA-5 (4).1 (i)

---

**CCI:** CCI-000900 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization ensures that approvals, consents, and detailed operational conditions regarding the use of foreign nationals to conduct maintenance and diagnostic activities on classified information systems are fully documented within Memoranda of Agreements.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): MA-5 (4) (b)
NIST: NIST SP 800-53 Revision 4 (v4): MA-5 (4) (b)
NIST: NIST SP 800-53A (v1): MA-5 (4).1 (ii)

---

**CCI:** CCI-002893 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-07-22
**Definition:** The organization ensures that non-escorted personnel performing maintenance activities not directly associated with the information system but in the physical proximity of the system, have required access authorization.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): MA-5 (5)

---

**CCI:** CCI-000903 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-18
**Definition:** The organization obtains maintenance support and/or spare parts for organization-defined information system components within an organization-defined time period of failure.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): MA-6
NIST: NIST SP 800-53 Revision 4 (v4): MA-6
NIST: NIST SP 800-53A (v1): MA-6.1 (iii)

---

**CCI:** CCI-002896 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-07-22
**Definition:** The organization defines the information system components for which it obtains maintenance support and/or spare parts.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): MA-6

---

**CCI:** CCI-002897 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-07-22
**Definition:** The organization defines a time period for obtaining maintenance support and/or spare parts for organization-defined information system components after a failure.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): MA-6

---

**CCI:** CCI-002898 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-07-22
**Definition:** The organization performs preventive maintenance on organization-defined information system components at organization-defined time intervals.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): MA-6 (1)

---

**CCI:** CCI-002899 **Status:** draft
**Contributor:** DISA FSO **Published** 2013-07-22

**Date:**

**Definition:** The organization defines information system components on which to perform preventive maintenance.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): MA-6 (1)

---

**CCI:** CCI-002900 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-22

**Definition:** The organization defines time intervals at which to perform preventive maintenance on organization-defined information system components.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): MA-6 (1)

---

**CCI:** CCI-002901 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-22

**Definition:** The organization performs predictive maintenance on organization-defined information system components at organization-defined intervals.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): MA-6 (2)

---

**CCI:** CCI-002902 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-22

**Definition:** The organization defines information system components on which to perform predictive maintenance.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): MA-6 (2)

---

**CCI:** CCI-002903 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-22

**Definition:** The organization defines time intervals at which to perform predictive maintenance on organization-defined information system components.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): MA-6 (2)

---

**CCI:** CCI-002904 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-22

**Definition:** The organization employs automated mechanisms to transfer predictive maintenance data to a computerized maintenance management system.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): MA-6 (3)

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000995 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization develops and documents a media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): MP-1 a<br>NIST: NIST SP 800-53 Revision 4 (v4): MP-1 a 1<br>NIST: NIST SP 800-53A (v1): MP-1.1 (i and ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000996 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization disseminates to organization-defined personnel or roles a media protection policy. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): MP-1 a<br>NIST: NIST SP 800-53 Revision 4 (v4): MP-1 a 1<br>NIST: NIST SP 800-53A (v1): MP-1.1 (iii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000999 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization develops and documents procedures to facilitate the implementation of the media protection policy and associated media protection controls. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): MP-1 b<br>NIST: NIST SP 800-53 Revision 4 (v4): MP-1 a 2<br>NIST: NIST SP 800-53A (v1): MP-1.1 (iv and v) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001000 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization disseminates to organization-defined personnel or roles procedures to facilitate the implementation of the media protection policy and associated media protection controls. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): MP-1 b<br>NIST: NIST SP 800-53 Revision 4 (v4): MP-1 a 2<br>NIST: NIST SP 800-53A (v1): MP-1.1 (vi) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002566 | **Status:** | draft |

| | | | |
|---|---|---|---|
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-09 |
| **Definition:** | The organization defines personnel or roles to whom a documented media protection policy and procedures will be disseminated. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): MP-1 a 1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000997 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization reviews and updates the current media protection policy in accordance with organization-defined frequency. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): MP-1 a<br>NIST: NIST SP 800-53 Revision 4 (v4): MP-1 b 1<br>NIST: NIST SP 800-53A (v1): MP-1.2 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000998 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization defines a frequency for reviewing and updating the current media protection policy. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): MP-1 a<br>NIST: NIST SP 800-53 Revision 4 (v4): MP-1 b 1<br>NIST: NIST SP 800-53A (v1): MP-1.2 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001001 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization reviews and updates the current media protection procedures in accordance with organization-defined frequency. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): MP-1 b<br>NIST: NIST SP 800-53 Revision 4 (v4): MP-1 b 2<br>NIST: NIST SP 800-53A (v1): MP-1.2 (iv) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001002 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization defines a frequency for reviewing and updating the current media protection procedures. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): MP-1 b | | |

| | | | |
|---|---|---|---|
| | NIST: NIST SP 800-53 Revision 4 (v4): MP-1 b 2<br>NIST: NIST SP 800-53A (v1): MP-1.2 (iii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001003 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization restricts access to organization-defined types of digital and/or non-digital media to organization-defined personnel or roles. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): MP-2<br>NIST: NIST SP 800-53 Revision 4 (v4): MP-2<br>NIST: NIST SP 800-53A (v1): MP-2.1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001004 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization defines types of digital and/or non-digital media for which the organization restricts access. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): MP-2<br>NIST: NIST SP 800-53 Revision 4 (v4): MP-2<br>NIST: NIST SP 800-53A (v1): MP-2.1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001005 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization defines personnel or roles from which to restrict access to organization-defined types of digital and/or non-digital media. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): MP-2<br>NIST: NIST SP 800-53 Revision 4 (v4): MP-2<br>NIST: NIST SP 800-53A (v1): MP-2.1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001010 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): MP-3 a<br>NIST: NIST SP 800-53 Revision 4 (v4): MP-3 a<br>NIST: NIST SP 800-53A (v1): MP-3.1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001011 | **Status:** | draft |

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization exempts organization-defined types of information system media from marking as long as the media remain within organization-defined controlled areas.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): MP-3 b
NIST: NIST SP 800-53 Revision 4 (v4): MP-3 b
NIST: NIST SP 800-53A (v1): MP-3.1 (iv)

---

**CCI:** CCI-001012 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization defines types of information system media to exempt from marking as long as the media remain within organization-defined controlled areas.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): MP-3 b
NIST: NIST SP 800-53 Revision 4 (v4): MP-3 b
NIST: NIST SP 800-53A (v1): MP-3.1 (iii)

---

**CCI:** CCI-001013 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization defines controlled areas where organization-defined types of information system media are exempt from being marked.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): MP-3 b
NIST: NIST SP 800-53 Revision 4 (v4): MP-3 b
NIST: NIST SP 800-53A (v1): MP-3.1 (iii)

---

**CCI:** CCI-001014 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization physically controls and securely stores organization-defined types of digital and/or non-digital media within organization-defined controlled areas.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): MP-4 a
NIST: NIST SP 800-53 Revision 4 (v4): MP-4 a
NIST: NIST SP 800-53A (v1): MP-4.1 (ii)

---

**CCI:** CCI-001015 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization defines types of digital and/or non-digital media to physically control and securely store within organization-defined controlled areas.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): MP-4 a
NIST: NIST SP 800-53 Revision 4 (v4): MP-4 a
NIST: NIST SP 800-53A (v1): MP-4.1 (i)

---

**CCI:** CCI-001016 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization defines controlled areas where organization-defined types of digital and/or non-digital media are physically controlled and securely stored.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): MP-4 a
NIST: NIST SP 800-53 Revision 4 (v4): MP-4 a
NIST: NIST SP 800-53A (v1): MP-4.1 (i)

---

**CCI:** CCI-001018 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): MP-4 b
NIST: NIST SP 800-53 Revision 4 (v4): MP-4 b
NIST: NIST SP 800-53A (v1): MP-4.1 (iii)

---

**CCI:** CCI-001007 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization employs automated mechanisms to restrict access to media storage areas.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): MP-2 (1)
NIST: NIST SP 800-53 Revision 4 (v4): MP-4 (2)
NIST: NIST SP 800-53A (v1): MP-2 (1).1 (i)

---

**CCI:** CCI-001008 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization employs automated mechanisms to audit access attempts and access granted to media storage areas.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): MP-2 (1)
NIST: NIST SP 800-53 Revision 4 (v4): MP-4 (2)
NIST: NIST SP 800-53A (v1): MP-2 (1).1 (ii)

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001020 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization protects and controls organization-defined types of information system media during transport outside of controlled areas using organization-defined security safeguards. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): MP-5 a<br>NIST: NIST SP 800-53 Revision 4 (v4): MP-5 a<br>NIST: NIST SP 800-53A (v1): MP-5.1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001021 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization defines types of information system media protected and controlled during transport outside of controlled areas. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): MP-5 a<br>NIST: NIST SP 800-53 Revision 4 (v4): MP-5 a<br>NIST: NIST SP 800-53A (v1): MP-5 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001022 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization defines security safeguards to be used to protect and control organization-defined types of information system media during transport outside of controlled areas. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): MP-5 a<br>NIST: NIST SP 800-53 Revision 4 (v4): MP-5 a<br>NIST: NIST SP 800-53A (v1): MP-5.1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001023 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization maintains accountability for information system media during transport outside of controlled areas. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): MP-5 b<br>NIST: NIST SP 800-53 Revision 4 (v4): MP-5 b<br>NIST: NIST SP 800-53A (v1): MP-5.1 (iii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001025 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |

**Definition:** The organization documents activities associated with the transport of information system media.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): MP-5 (2)
NIST: NIST SP 800-53 Revision 4 (v4): MP-5 c
NIST: NIST SP 800-53A (v1): MP-5 (2).1

---

**CCI:** CCI-001024 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization restricts the activities associated with the transport of information system media to authorized personnel.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): MP-5 c
NIST: NIST SP 800-53 Revision 4 (v4): MP-5 d
NIST: NIST SP 800-53A (v1): MP-5.1 (v)

---

**CCI:** CCI-001026 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization employs an identified custodian during transport of information system media outside of controlled areas.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): MP-5 (3)
NIST: NIST SP 800-53 Revision 4 (v4): MP-5 (3)
NIST: NIST SP 800-53A (v1): MP-5 (3).1

---

**CCI:** CCI-001027 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The information system implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): MP-5 (4)
NIST: NIST SP 800-53 Revision 4 (v4): MP-5 (4)
NIST: NIST SP 800-53A (v1): MP-5 (4).1

---

**CCI:** CCI-001028 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization sanitizes organization-defined information system media prior to disposal, release out of organizational control, or release for reuse using organization-defined sanitization techniques and procedures in accordance with applicable federal and organizational standards and policies.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): MP-6
NIST: NIST SP 800-53 Revision 4 (v4): MP-6 a
NIST: NIST SP 800-53A (v1): MP-6.1 (ii)

---

**CCI:** CCI-002578 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-09

**Definition:** The organization defines information system media to sanitize prior to disposal, release out of organizational control, or release for reuse using organization-defined sanitization techniques and procedures in accordance with applicable federal and organizational standards and policies.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): MP-6 a

---

**CCI:** CCI-002579 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-09

**Definition:** The organization defines the sanitization techniques and procedures to be used to sanitize organization-defined information system media prior to disposal, release out of organizational control, or release for reuse in accordance with applicable federal and organization standards and policies.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): MP-6 a

---

**CCI:** CCI-002580 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-09

**Definition:** The organization employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): MP-6 b

---

**CCI:** CCI-002567 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-09

**Definition:** The organization reviews and approves media sanitization.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): MP-6 (1)

---

**CCI:** CCI-002568 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-09

**Definition:** The organization tracks and documents media sanitization.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): MP-6 (1)

---

**CCI:** CCI-002569 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-09

**Definition:** The organization verifies media sanitization.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): MP-6 (1)

---

**CCI:** CCI-002570 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-09

**Definition:** The organization reviews and approves media disposal actions.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): MP-6 (1)

---

**CCI:** CCI-002571 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-09

**Definition:** The organization tracks and documents media disposal actions.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): MP-6 (1)

---

**CCI:** CCI-002572 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-09

**Definition:** The organization verifies media disposal actions.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): MP-6 (1)

---

**CCI:** CCI-001030 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization tests sanitization equipment and procedures in accordance with the organization-defined frequency to verify that the intended sanitization is being achieved.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): MP-6 (2)
NIST: NIST SP 800-53 Revision 4 (v4): MP-6 (2)
NIST: NIST SP 800-53A (v1): MP-6 (2).1 (ii)

---

**CCI:** CCI-001031 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization defines a frequency for testing sanitization equipment and procedures to verify that the intended sanitization is being achieved.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): MP-6 (2)
NIST: NIST SP 800-53 Revision 4 (v4): MP-6 (2)
NIST: NIST SP 800-53A (v1): MP-6 (2).1 (i)

---

**CCI:** CCI-001032 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization applies nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the information system in accordance with organization-defined circumstances requiring sanitization of portable storage devices.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): MP-6 (3)
NIST: NIST SP 800-53 Revision 4 (v4): MP-6 (3)
NIST: NIST SP 800-53A (v1): MP-6 (3).1 (ii)

---

**CCI:** CCI-001033 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization defines circumstances requiring sanitization of portable storage devices prior to connecting such devices to the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): MP-6 (3)
NIST: NIST SP 800-53 Revision 4 (v4): MP-6 (3)
NIST: NIST SP 800-53A (v1): MP-6 (3).1 (i)

---

**CCI:** CCI-002573 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-09

**Definition:** The organization enforces dual authorization for the sanitization of organization-defined information system media.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): MP-6 (7)

---

**CCI:** CCI-002574 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-09

**Definition:** The organization defines the information system media that dual authorization is enforced for sanitization.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): MP-6 (7)

---

**CCI:** CCI-002575 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-09

**Definition:** The organization defines information systems, system components, or devices from which information is to be purged/wiped, either remotely or under the organization-defined conditions.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): MP-6 (8)

---

**CCI:** CCI-002576 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-09

**Definition:** The organization defines conditions under which information from organization-defined information systems, system components, or devices should be purged/wiped.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): MP-6 (8)

---

**CCI:** CCI-002577 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-09

**Definition:** The organization provides the capability to purge/wipe information from organization-defined information systems, system components, or devices either remotely or under organization-defined conditions.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): MP-6 (8)

---

**CCI:** CCI-002581 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-09

**Definition:** The organization defines the types of information system media to restrict or prohibit on organization-defined information systems or system components using organization-defined security safeguards.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): MP-7

---

**CCI:** CCI-002582 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-09

**Definition:** The organization defines the information systems or system components on which to restrict or prohibit the use of organization-defined types of information system media using organization-defined security safeguards.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): MP-7

---

**CCI:** CCI-002583 **Status:** draft

**Contributor:** DISA FSO **Published** 2013-07-09

**Date:**

**Definition:** The organization defines the security safeguards to use for restricting or prohibiting the use of organization-defined types of information system media on organization-defined information systems or system components.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): MP-7

---

**CCI:** CCI-002584 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-09

**Definition:** The organization restricts or prohibits the use of organization-defined types of information system media on organization-defined information systems or system components using organization-defined security safeguards.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): MP-7

---

**CCI:** CCI-002585 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-09

**Definition:** The organization prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): MP-7 (1)

---

**CCI:** CCI-002586 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-09

**Definition:** The organization prohibits the use of sanitization-resistant media in organizational information systems.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): MP-7 (2)

---

**CCI:** CCI-002595 **Status:** deprecated

**Contributor:** DISA FSO **Published Date:** 2013-07-09

**Definition:** The organization establishes an organization-defined information system media downgrading process that includes employing downgrading mechanisms with organization-defined strength and integrity.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): MP-8 a

---

**CCI:** CCI-002596 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-09

**Definition:** The organization establishes and defines an information system media downgrading

|  |  |  |  |
|---|---|---|---|
|  | process that includes employing downgrading mechanisms with organization-defined strength and integrity. |  |  |
| **Type:** | policy |  |  |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): MP-8 a |  |  |

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-002597 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-09 |
| **Definition:** | The organization defines strength and integrity for downgrading mechanisms to establish an organization-defined information system media downgrading process. |  |  |
| **Type:** | policy |  |  |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): MP-8 a |  |  |

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-002598 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-09 |
| **Definition:** | The organization ensures that the information system media downgrading process is commensurate with the security category and/or classification level of the information to be removed and the access authorizations of the potential recipients of the downgraded information. |  |  |
| **Type:** | policy |  |  |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): MP-8 b |  |  |

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-002599 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-09 |
| **Definition:** | The organization defines and identifies the information system media requiring downgrading. |  |  |
| **Type:** | policy |  |  |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): MP-8 c |  |  |

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-002600 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-09 |
| **Definition:** | The organization downgrades the identified information system media using the established process. |  |  |
| **Type:** | policy |  |  |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): MP-8 d |  |  |

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-002587 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-09 |
| **Definition:** | The organization documents information system media downgrading actions. |  |  |
| **Type:** | policy |  |  |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): MP-8 (1) |  |  |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002588 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-09 |
| **Definition:** | The organization employs organization-defined tests of downgrading equipment in accordance with organization-defined frequency. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): MP-8 (2) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002589 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-09 |
| **Definition:** | The organization employs procedures to verify correct performance of organization-defined tests of downgrading equipment in accordance with organization-defined frequency. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): MP-8 (2) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002590 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-09 |
| **Definition:** | The organization defines tests to employ for downgrading equipment. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): MP-8 (2) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002591 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-09 |
| **Definition:** | The organization defines the frequency with which to employ tests of downgrading equipment and procedures to verify correct performance. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): MP-8 (2) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002592 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-09 |
| **Definition:** | The organization defines Controlled Unclassified Information (CUI). | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): MP-8 (3) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002593 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-09 |
| **Definition:** | The organization downgrades information system media containing organization-defined Controlled Unclassified Information (CUI) prior to public release in accordance with applicable federal and organizational standards and policies. | | |

| | | | |
|---|---|---|---|
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): MP-8 (3) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002594 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-09 |
| **Definition:** | The organization downgrades information system media containing classified information prior to release to individuals without required access authorizations in accordance with NSA standards and policies. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): MP-8 (4) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000904 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization develops and documents a physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PE-1 a<br>NIST: NIST SP 800-53 Revision 4 (v4): PE-1 a 1<br>NIST: NIST SP 800-53A (v1): PE-1.1 (i and ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000905 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization disseminates a physical and environmental protection policy to organization-defined personnel or roles. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PE-1 a<br>NIST: NIST SP 800-53 Revision 4 (v4): PE-1 a 1<br>NIST: NIST SP 800-53A (v1): PE-1.1 (iii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000908 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization develops and documents procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PE-1 b<br>NIST: NIST SP 800-53 Revision 4 (v4): PE-1 a 2<br>NIST: NIST SP 800-53A (v1): PE-1.1 (iv and v) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000909 | **Status:** | draft |

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization disseminates physical and environmental protection procedures to organization-defined personnel or roles.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PE-1 b
NIST: NIST SP 800-53 Revision 4 (v4): PE-1 a 2
NIST: NIST SP 800-53A (v1): PE-1.1 (vi)

---

**CCI:** CCI-002908 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-08-27

**Definition:** The organization defines the personnel or roles to whom a physical and environmental protection policy is disseminated.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PE-1 a 1

---

**CCI:** CCI-002909 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-08-27

**Definition:** The organization defines the personnel or roles to whom the physical and environmental protection procedures are disseminated.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PE-1 a 2

---

**CCI:** CCI-000906 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization reviews and updates the current physical and environmental protection policy in accordance with organization-defined frequency.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PE-1 a
NIST: NIST SP 800-53 Revision 4 (v4): PE-1 b 1
NIST: NIST SP 800-53A (v1): PE-1.2 (ii)

---

**CCI:** CCI-000907 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization defines the frequency with which to review and update the physical and environmental protection policy.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PE-1 a
NIST: NIST SP 800-53 Revision 4 (v4): PE-1 b 1
NIST: NIST SP 800-53A (v1): PE-1.2 (i)

---

**CCI:** CCI-000910 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization reviews and updates the current physical and environmental protection procedures in accordance with organization-defined frequency.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): PE-1 b
NIST: NIST SP 800-53 Revision 4 (v4): PE-1 b 2
NIST: NIST SP 800-53A (v1): PE-1.2 (iv)

---

**CCI:** CCI-000911 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization defines the frequency with which to review and update the physical and environmental protection procedures.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): PE-1 b
NIST: NIST SP 800-53 Revision 4 (v4): PE-1 b 2
NIST: NIST SP 800-53A (v1): PE-1.2 (iii)

---

**CCI:** CCI-000912 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization develops a list of individuals with authorized access to the facility where the information system resides.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): PE-2 a
NIST: NIST SP 800-53 Revision 4 (v4): PE-2 a
NIST: NIST SP 800-53A (v1): PE-2 (1).1 (i)

---

**CCI:** CCI-002910 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-08-27
**Definition:** The organization approves a list of individuals with authorized access to the facility where the information system resides.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): PE-2 a

---

**CCI:** CCI-002911 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-08-27
**Definition:** The organization maintains a list of individuals with authorized access to the facility where the information system resides.
**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PE-2 a

---

**CCI:** CCI-000913 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization issues authorization credentials for facility access.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PE-2 b
NIST: NIST SP 800-53 Revision 4 (v4): PE-2 b
NIST: NIST SP 800-53A (v1): PE-2.1 (iii)

---

**CCI:** CCI-000914 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization reviews the access list detailing authorized facility access by individuals in accordance with organization-defined frequency.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PE-2 c
NIST: NIST SP 800-53 Revision 4 (v4): PE-2 c
NIST: NIST SP 800-53A (v1): PE-2.2 (ii)

---

**CCI:** CCI-000915 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization defines the frequency with which to review the access list detailing authorized facility access by individuals.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PE-2 c
NIST: NIST SP 800-53 Revision 4 (v4): PE-2 c
NIST: NIST SP 800-53A (v1): PE-2.2 (i)

---

**CCI:** CCI-001635 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2010-05-12

**Definition:** The organization removes individuals from the facility access list when access is no longer required.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PE-2 c
NIST: NIST SP 800-53 Revision 4 (v4): PE-2 d
NIST: NIST SP 800-53A (v1): PE-2.2 (iii)

---

**CCI:** CCI-000916 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization authorizes physical access to the facility where the information system resides based on position or role.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PE-2 (1)
NIST: NIST SP 800-53 Revision 4 (v4): PE-2 (1)
NIST: NIST SP 800-53A (v1): PE-2 (1).1 (ii)

---

**CCI:** CCI-000917 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization requires two forms of identification from an organization-defined list of acceptable forms of identification for visitor access to the facility where the information system resides.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PE-2 (2)
NIST: NIST SP 800-53 Revision 4 (v4): PE-2 (2)
NIST: NIST SP 800-53A (v1): PE-2 (2).1

---

**CCI:** CCI-002912 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-08-27

**Definition:** The organization defines a list of acceptable forms of identification for visitor access to the facility where the information system resides.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PE-2 (2)

---

**CCI:** CCI-002913 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-08-27

**Definition:** The organization restricts unescorted access to the facility where the information system resides to personnel with one or more of the following: security clearances for all information contained within the system; formal access authorizations for all information contained within the system; need for access to all information contained within the system; organization-defined credentials.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PE-2 (3)

---

**CCI:** CCI-002914 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-08-27

**Definition:** The organization defines the credentials required for personnel to have unescorted access to the facility where the information system resides.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PE-2 (3)

---

**CCI:** CCI-000919 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization enforces physical access authorizations at organization-defined entry/exit points to the facility where the information system resides.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PE-3 a

NIST: NIST SP 800-53 Revision 4 (v4): PE-3 a

NIST: NIST SP 800-53A (v1): PE-3.1 (i)

---

**CCI:** CCI-000920 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization verifies individual access authorizations before granting access to the facility.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PE-3 b

NIST: NIST SP 800-53 Revision 4 (v4): PE-3 a 1

NIST: NIST SP 800-53A (v1): PE-3.1 (ii)

---

**CCI:** CCI-000921 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization controls ingress/egress to the facility where the information system resides using one or more organization-defined physical access control systems/devices or guards.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PE-3 c

NIST: NIST SP 800-53 Revision 4 (v4): PE-3 a 2

NIST: NIST SP 800-53A (v1): PE-3.1 (iii)

---

**CCI:** CCI-002915 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-08-27

**Definition:** The organization defines the entry/exit points to the facility where the information system resides.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PE-3 a

---

**CCI:** CCI-002916 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-08-27

**Definition:** The organization defines the physical access control systems/devices or guards that control ingress/egress to the facility where the information system resides.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PE-3 a 2

---

**CCI:** CCI-002917 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-08-27

**Definition:** The organization maintains physical access audit logs for organization-defined entry/exit points to the facility where the information system resides.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PE-3 b

---

**CCI:** CCI-002918 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-08-27

**Definition:** The organization defines entry/exit points to the facility where the information system resides that require physical access audit logs be maintained.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PE-3 b

---

**CCI:** CCI-002919 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-08-27

**Definition:** The organization provides organization-defined security safeguards to control access to areas within the facility where the information system resides officially designated as publicly accessible.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PE-3 c

---

**CCI:** CCI-002920 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-08-27

**Definition:** The organization defines security safeguards to control access to areas within the facility where the information system resides officially designated as publicly accessible.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PE-3 c

---

**CCI:** CCI-002921 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-08-27

**Definition:** The organization escorts visitors in the facility where the information system resides during organization-defined circumstances requiring visitor escorts.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PE-3 d

---

**CCI:** CCI-002922 **Status:** draft

| | | | |
|---|---|---|---|
| **Contributor:** | DISA FSO | **Published Date:** | 2013-08-27 |
| **Definition:** | The organization defines circumstances requiring visitor escorts in the facility where the information system resides. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PE-3 d | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002923 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-08-27 |
| **Definition:** | The organization monitors visitor activity in the facility where the information system resides during organization-defined circumstances requiring visitor monitoring. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PE-3 d | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002924 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-08-27 |
| **Definition:** | The organization defines circumstances requiring visitor monitoring in the facility where the information system resides. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PE-3 d | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000923 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization secures keys, combinations, and other physical access devices. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PE-3 e<br>NIST: NIST SP 800-53 Revision 4 (v4): PE-3 e<br>NIST: NIST SP 800-53A (v1): PE-3.1 (v) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000924 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization inventories organization-defined physical access devices on an organization-defined frequency. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PE-3 f<br>NIST: NIST SP 800-53 Revision 4 (v4): PE-3 f<br>NIST: NIST SP 800-53A (v1): PE-3.2 (ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000925 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published** | 2009-09-21 |

**Date:**

**Definition:** The organization defines the frequency for conducting inventories of organization-defined physical access devices.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PE-3 f
NIST: NIST SP 800-53 Revision 4 (v4): PE-3 f
NIST: NIST SP 800-53A (v1): PE-3.2 (i)

---

**CCI:** CCI-002925

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2013-08-27

**Definition:** The organization defines the physical access devices to inventory.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PE-3 f

---

**CCI:** CCI-000926

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2009-09-21

**Definition:** The organization changes combinations and keys in accordance with organization-defined frequency and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PE-3 g
NIST: NIST SP 800-53 Revision 4 (v4): PE-3 g
NIST: NIST SP 800-53A (v1): PE-3.2 (iv)

---

**CCI:** CCI-000927

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2009-09-21

**Definition:** The organization defines a frequency for changing combinations and keys.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PE-3 g
NIST: NIST SP 800-53 Revision 4 (v4): PE-3 g
NIST: NIST SP 800-53A (v1): PE-3.2 (iii)

---

**CCI:** CCI-000928

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2009-09-21

**Definition:** The organization enforces physical access authorizations to the information system in addition to the physical access controls for the facility where the information system resides at organization-defined physical spaces containing one or more components of the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PE-3 (1)

NIST: NIST SP 800-53 Revision 4 (v4): PE-3 (1)
NIST: NIST SP 800-53A (v1): PE-3 (1).1

---

**CCI:** CCI-002926
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2013-08-27
**Definition:** The organization defines the physical spaces containing one or more components of the information system that require physical access authorizations and controls at the facility where the information system resides.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): PE-3 (1)

---

**CCI:** CCI-000929
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2009-09-21
**Definition:** The organization performs security checks in accordance with organization-defined frequency at the physical boundary of the facility or information system for unauthorized exfiltration of information or removal of information system components.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): PE-3 (2)
NIST: NIST SP 800-53 Revision 4 (v4): PE-3 (2)
NIST: NIST SP 800-53A (v1): PE-3 (2).1

---

**CCI:** CCI-002927
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2013-08-27
**Definition:** The organization defines the frequency with which to perform security checks at the physical boundary of the facility or information system for unauthorized exfiltration of information or removal of information system components.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): PE-3 (2)

---

**CCI:** CCI-000930
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2009-09-21
**Definition:** The organization employs guards and/or alarms to monitor every physical access point to the facility where the information system resides 24 hours per day, 7 days per week.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): PE-3 (3)
NIST: NIST SP 800-53 Revision 4 (v4): PE-3 (3)
NIST: NIST SP 800-53A (v1): PE-3 (3).1

---

**CCI:** CCI-000931
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2009-09-21

**Definition:** The organization uses lockable physical casings to protect organization-defined information system components from unauthorized physical access.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PE-3 (4)
NIST: NIST SP 800-53 Revision 4 (v4): PE-3 (4)
NIST: NIST SP 800-53A (v1): PE-3 (4).1 (ii)

---

**CCI:** CCI-000932 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization defines information system components to be protected from unauthorized physical access using lockable physical casings.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PE-3 (4)
NIST: NIST SP 800-53 Revision 4 (v4): PE-3 (4)
NIST: NIST SP 800-53A (v1): PE-3 (4).1 (i)

---

**CCI:** CCI-000933 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization employs organization-defined security safeguards to deter and/or prevent physical tampering or alteration of organization-defined hardware components within the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PE-3 (5)
NIST: NIST SP 800-53 Revision 4 (v4): PE-3 (5)
NIST: NIST SP 800-53A (v1): PE-3 (5).1

---

**CCI:** CCI-002928 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-08-27

**Definition:** The organization defines security safeguards to detect and prevent physical tampering or alteration of organization-defined hardware components within the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PE-3 (5)

---

**CCI:** CCI-002929 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-08-27

**Definition:** The organization defines hardware components within the information system for which to employ organization-defined security safeguards to detect and prevent physical tampering or alteration.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PE-3 (5)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000934 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |

**Definition:** The organization employs a penetration testing process that includes unannounced attempts to bypass or circumvent security controls associated with physical access points to the facility on an organization-defined frequency.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PE-3 (6)
NIST: NIST SP 800-53 Revision 4 (v4): PE-3 (6)
NIST: NIST SP 800-53A (v1): PE-3 (6).1 (ii)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000935 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |

**Definition:** The organization defines the frequency of unannounced attempts to be included in a penetration testing process to bypass or circumvent security controls associated with physical access points to the facility.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PE-3 (6)
NIST: NIST SP 800-53 Revision 4 (v4): PE-3 (6)
NIST: NIST SP 800-53A (v1): PE-3 (6).1 (i)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000936 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |

**Definition:** The organization controls physical access to organization-defined information system distribution and transmission lines within organizational facilities using organization-defined security safeguards.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PE-4
NIST: NIST SP 800-53 Revision 4 (v4): PE-4
NIST: NIST SP 800-53A (v1): PE-4.1

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002930 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-08-27 |

**Definition:** The organization defines information system distribution and transmission lines within organizational facilities to control physical access to using organization-defined security safeguards.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PE-4

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002931 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-08-27 |

| | | | |
|---|---|---|---|
| **Definition:** | The organization defines security safeguards to control physical access to organization-defined information system distribution and transmission lines within organizational facilities. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PE-4 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000937 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PE-5<br>NIST: NIST SP 800-53 Revision 4 (v4): PE-5<br>NIST: NIST SP 800-53A (v1): PE-5.1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002932 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-08-27 |
| **Definition:** | The organization controls physical access to output from organization-defined output devices. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PE-5 (1) (a) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002933 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-08-27 |
| **Definition:** | The organization defines output devices for which physical access to output is controlled. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PE-5 (1) (a) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002934 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-08-27 |
| **Definition:** | The organization ensures that only authorized individuals receive output from organization-defined output devices. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PE-5 (1) (b) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002935 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-08-27 |
| **Definition:** | The information system controls physical access to output from organization-defined output devices. | | |
| **Type:** | policy | | |

| | | | |
|---|---|---|---|
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PE-5 (2) (a) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002936 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-08-27 |
| **Definition:** | The information system links individual identity to receipt of output from organization-defined output devices. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PE-5 (2) (b) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002937 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-08-27 |
| **Definition:** | The organization marks organization-defined information system output devices indicating the appropriate security marking of the information permitted to be output from the device. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PE-5 (3) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002938 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-08-27 |
| **Definition:** | The organization defines the information system output devices marked indicating the appropriate security marking of the information permitted to be output from the device. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PE-5 (3) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002939 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-08-27 |
| **Definition:** | The organization monitors physical access to the facility where the information system resides to detect and respond to physical security incidents. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PE-6 a | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000939 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization reviews physical access logs in accordance with organization-defined frequency. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PE-6 b<br>NIST: NIST SP 800-53 Revision 4 (v4): PE-6 b<br>NIST: NIST SP 800-53A (v1): PE-6.1 (iii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000940 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization defines a frequency for reviewing physical access logs. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PE-6 b<br>NIST: NIST SP 800-53 Revision 4 (v4): PE-6 b<br>NIST: NIST SP 800-53A (v1): PE-6.1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002940 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-08-27 |
| **Definition:** | The organization reviews physical access logs upon occurrence of organization-defined events or potential indications of events. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PE-6 b | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002941 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-08-27 |
| **Definition:** | The organization defines events or potential indications of events requiring review of physical access logs. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PE-6 b | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000941 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization coordinates results of reviews and investigations with the organization's incident response capability. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PE-6 c<br>NIST: NIST SP 800-53 Revision 4 (v4): PE-6 c<br>NIST: NIST SP 800-53A (v1): PE-6.1 (iv) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000942 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization monitors physical intrusion alarms and surveillance equipment. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PE-6 (1)<br>NIST: NIST SP 800-53 Revision 4 (v4): PE-6 (1)<br>NIST: NIST SP 800-53A (v1): PE-6 (1).1 | | |

**CCI:** CCI-002942 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-08-27
**Definition:** The organization employs automated mechanisms to recognize organization-defined classes/types of intrusions.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): PE-6 (2)

---

**CCI:** CCI-002943 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-08-27
**Definition:** The organization defines classes/types of intrusions to recognize using automated mechanisms.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): PE-6 (2)

---

**CCI:** CCI-002944 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-08-27
**Definition:** The organization employs automated mechanisms to initiate organization-defined response actions to organization-defined classes/types of intrusions.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): PE-6 (2)

---

**CCI:** CCI-002945 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-08-27
**Definition:** The organization defines response actions to initiate when organization-defined classes/types of intrusions are recognized.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): PE-6 (2)

---

**CCI:** CCI-002946 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-08-27
**Definition:** The organization employs video surveillance of organization-defined operational areas.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): PE-6 (3)

---

**CCI:** CCI-002947 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-08-27
**Definition:** The organization defines the operational areas in which to employ video surveillance.
**Type:** policy

| | | | |
|---|---|---|---|
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PE-6 (3) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002948 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-08-27 |
| **Definition:** | The organization retains video surveillance recordings for an organization-defined time period. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PE-6 (3) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002949 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-08-27 |
| **Definition:** | The organization defines the time period to retain video surveillance recordings. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PE-6 (3) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002950 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-08-27 |
| **Definition:** | The organization monitors physical access to the information system in addition to the physical access monitoring of the facility as organization-defined physical spaces containing one or more components of the information system. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PE-6 (4) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002951 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-08-27 |
| **Definition:** | The organization defines physical spaces containing one or more components of the information system in which physical access is monitored. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PE-6 (4) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000947 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization maintains visitor access records to the facility where the information system resides for an organization-defined time period. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PE-8 a<br>NIST: NIST SP 800-53 Revision 4 (v4): PE-8 a<br>NIST: NIST SP 800-53A (v1): PE-8.1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002952 | **Status:** | draft |

**Contributor:** DISA FSO **Published Date:** 2013-08-27

**Definition:** The organization defines the time period to maintain visitor access records to the facility where the information system resides.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PE-8 a

---

**CCI:** CCI-000948 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization reviews visitor access records in accordance with organization-defined frequency.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PE-8 b
NIST: NIST SP 800-53 Revision 4 (v4): PE-8 b
NIST: NIST SP 800-53A (v1): PE-8.1 (ii)

---

**CCI:** CCI-000949 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization defines the frequency with which to review the visitor access records for the facility where the information system resides.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PE-8 b
NIST: NIST SP 800-53 Revision 4 (v4): PE-8 b
NIST: NIST SP 800-53A (v1): PE-8.1 (ii)

---

**CCI:** CCI-000950 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization employs automated mechanisms to facilitate the maintenance and review of access records.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PE-8 (1)
NIST: NIST SP 800-53 Revision 4 (v4): PE-8 (1)
NIST: NIST SP 800-53A (v1): PE-8 (1).1

---

**CCI:** CCI-000952 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization protects power equipment and power cabling for the information system from damage and destruction.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PE-9

|  |  |  |  |
|---|---|---|---|
|  | NIST: NIST SP 800-53 Revision 4 (v4): PE-9<br>NIST: NIST SP 800-53A (v1): PE-9.1 |  |  |

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-002953 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-08-27 |
| **Definition:** | The organization employs redundant power cabling paths that are physically separated by an organization-defined distance. |  |  |
| **Type:** | policy |  |  |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PE-9 (1) |  |  |

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-002954 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-08-27 |
| **Definition:** | The organization defines the distance by which to physically separate redundant power cabling paths. |  |  |
| **Type:** | policy |  |  |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PE-9 (1) |  |  |

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-000954 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization employs automatic voltage controls for organization-defined critical information system components. |  |  |
| **Type:** | policy |  |  |
| **References:** | NIST: NIST SP 800-53 (v3): PE-9 (2)<br>NIST: NIST SP 800-53 Revision 4 (v4): PE-9 (2)<br>NIST: NIST SP 800-53A (v1): PE-9 (2).1 (ii) |  |  |

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-000955 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization defines critical information system components that require automatic voltage controls. |  |  |
| **Type:** | policy |  |  |
| **References:** | NIST: NIST SP 800-53 (v3): PE-9 (2)<br>NIST: NIST SP 800-53 Revision 4 (v4): PE-9 (2)<br>NIST: NIST SP 800-53A (v1): PE-9 (2).1 (i) |  |  |

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-000956 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization provides the capability of shutting off power to the information system or individual system components in emergency situations. |  |  |

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PE-10 a
NIST: NIST SP 800-53 Revision 4 (v4): PE-10 a
NIST: NIST SP 800-53A (v1): PE-10.1 (i)

---

**CCI:** CCI-000957 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization places emergency shutoff switches or devices in an organization-defined location by information system or system component to facilitate safe and easy access for personnel.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PE-10 b
NIST: NIST SP 800-53 Revision 4 (v4): PE-10 b
NIST: NIST SP 800-53A (v1): PE-10.1 (iii)

---

**CCI:** CCI-000958 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization defines a location for emergency shutoff switches or devices by information system or system component.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PE-10 b
NIST: NIST SP 800-53 Revision 4 (v4): PE-10 b
NIST: NIST SP 800-53A (v1): PE-10.1 (ii)

---

**CCI:** CCI-000959 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization protects emergency power shutoff capability from unauthorized activation.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PE-10 c
NIST: NIST SP 800-53 Revision 4 (v4): PE-10 c
NIST: NIST SP 800-53A (v1): PE-10.1 (iv)

---

**CCI:** CCI-002955 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-08-29

**Definition:** The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system and/or transition of the information system to long-term alternate power in the event of a primary power source loss.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PE-11

---

**CCI:** CCI-000961 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): PE-11 (1)
NIST: NIST SP 800-53 Revision 4 (v4): PE-11 (1)
NIST: NIST SP 800-53A (v1): PE-11 (1).1

---

**CCI:** CCI-002956 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-08-29
**Definition:** The organization provides a long-term alternate power supply for the information system that is self-contained.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): PE-11 (2) (a)

---

**CCI:** CCI-002957 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-08-29
**Definition:** The organization provides a long-term alternate power supply for the information system that is not reliant on external power generation.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): PE-11 (2) (b)

---

**CCI:** CCI-002958 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-08-29
**Definition:** The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability or full operational capability in the event of an extended loss of the primary power source.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): PE-11 (2) (c)

---

**CCI:** CCI-000963 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): PE-12
NIST: NIST SP 800-53 Revision 4 (v4): PE-12

NIST: NIST SP 800-53A (v1): PE-12.1 (i) (ii)(iii)

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002959 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-08-29 |
| **Definition:** | The organization provides emergency lighting for all areas within the facility supporting essential missions. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PE-12 (1) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002960 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-08-29 |
| **Definition:** | The organization provides emergency lighting for all areas within the facility supporting essential business functions. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PE-12 (1) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000965 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PE-13<br>NIST: NIST SP 800-53 Revision 4 (v4): PE-13<br>NIST: NIST SP 800-53A (v1): PE-13.1 (i) (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002961 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-08-29 |
| **Definition:** | The organization employs fire detection devices/systems for the information system that activate automatically. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PE-13 (1) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002962 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-08-29 |
| **Definition:** | The organization employs fire detection devices/systems for the information system that automatically activate to notify organization-defined personnel or roles and organization-defined emergency responders in the event of a fire. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PE-13 (1) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002963 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-08-29 |
| **Definition:** | The organization defines the personnel or roles to be notified in the event of a fire. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PE-13 (1) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002964 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-08-29 |
| **Definition:** | The organization defines the emergency responders to be notified in the event of a fire. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PE-13 (1) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002965 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-08-29 |
| **Definition:** | The organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to organization-defined personnel or roles and organization-defined emergency responders. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PE-13 (2) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002966 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-08-29 |
| **Definition:** | The organization defines the personnel or roles to be automatically notified of any activation of fire suppression devices/systems for the information system. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PE-13 (2) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002967 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-08-29 |
| **Definition:** | The organization defines the emergency responders to be automatically notified of any activation of fire suppression devices/systems for the information system. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PE-13 (2) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000968 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis. | | |
| **Type:** | policy | | |

**References:** NIST: NIST SP 800-53 (v3): PE-13 (3)
NIST: NIST SP 800-53 Revision 4 (v4): PE-13 (3)
NIST: NIST SP 800-53A (v1): PE-13 (3).1

---

**CCI:** CCI-002968 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-08-29
**Definition:** The organization ensures that the facility undergoes, on an organization-defined frequency, fire protection inspections by authorized and qualified inspectors.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): PE-13 (4)

---

**CCI:** CCI-002969 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-08-29
**Definition:** The organization defines a frequency with which the facility undergoes fire protection inspections.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): PE-13 (4)

---

**CCI:** CCI-002970 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-08-29
**Definition:** The organization resolves deficiencies identified during facility fire protection inspections within an organization-defined time period.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): PE-13 (4)

---

**CCI:** CCI-002971 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-08-29
**Definition:** The organization defines the time period within which to resolve deficiencies identified during facility fire protection inspections.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): PE-13 (4)

---

**CCI:** CCI-000971 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization maintains temperature and humidity levels within the facility where the information system resides at organization-defined acceptable levels.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): PE-14 a
NIST: NIST SP 800-53 Revision 4 (v4): PE-14 a

NIST: NIST SP 800-53A (v1): PE-14.1 (ii)

---

**CCI:** CCI-000972 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization defines acceptable temperature and humidity levels to be maintained within the facility where the information system resides.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PE-14 a

NIST: NIST SP 800-53 Revision 4 (v4): PE-14 a

NIST: NIST SP 800-53A (v1): PE-14.1 (i)

---

**CCI:** CCI-000973 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization monitors temperature and humidity levels in accordance with organization-defined frequency.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PE-14 b

NIST: NIST SP 800-53 Revision 4 (v4): PE-14 b

NIST: NIST SP 800-53A (v1): PE-14.1 (iv)

---

**CCI:** CCI-000974 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization defines a frequency for monitoring temperature and humidity levels.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PE-14 b

NIST: NIST SP 800-53 Revision 4 (v4): PE-14 b

NIST: NIST SP 800-53A (v1): PE-14.1 (iii)

---

**CCI:** CCI-000975 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization employs automatic temperature and humidity controls in the facility to prevent fluctuations potentially harmful to the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PE-14 (1)

NIST: NIST SP 800-53 Revision 4 (v4): PE-14 (1)

NIST: NIST SP 800-53A (v1): PE-14 (1).1

---

**CCI:** CCI-000976 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization employs temperature and humidity monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PE-14 (2)
NIST: NIST SP 800-53 Revision 4 (v4): PE-14 (2)
NIST: NIST SP 800-53A (v1): PE-14 (2).1

---

**CCI:** CCI-000977 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PE-15
NIST: NIST SP 800-53 Revision 4 (v4): PE-15
NIST: NIST SP 800-53A (v1): PE-15.1 (i)

---

**CCI:** CCI-000978 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are working properly.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PE-15
NIST: NIST SP 800-53 Revision 4 (v4): PE-15
NIST: NIST SP 800-53A (v1): PE-15.1 (i)

---

**CCI:** CCI-000979 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** Key personnel have knowledge of the master water shutoff or isolation valves.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PE-15
NIST: NIST SP 800-53 Revision 4 (v4): PE-15
NIST: NIST SP 800-53A (v1): PE-15.1 (ii)

---

**CCI:** CCI-002972 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-08-29

**Definition:** The organization employs automated mechanisms to detect the presence of water in the vicinity of the information system and alerts organization-defined personnel or roles.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PE-15 (1)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002973 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-08-29 |
| **Definition:** | The organization defines the personnel or roles to be alerted when automated mechanisms detect the presence of water in the vicinity of the information system. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PE-15 (1) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000981 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization authorizes organization-defined types of information system components entering and exiting the facility. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PE-16<br>NIST: NIST SP 800-53 Revision 4 (v4): PE-16<br>NIST: NIST SP 800-53A (v1): PE-16.1 (ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000982 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization monitors organization-defined types of information system components entering and exiting the facility. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PE-16<br>NIST: NIST SP 800-53 Revision 4 (v4): PE-16<br>NIST: NIST SP 800-53A (v1): PE-16.1 (ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000983 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization controls organization-defined types of information system components entering and exiting the facility. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PE-16<br>NIST: NIST SP 800-53 Revision 4 (v4): PE-16<br>NIST: NIST SP 800-53A (v1): PE-16.1 (ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000984 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization maintains records of information system components entering and exiting the facility. | | |
| **Type:** | policy | | |

**References:** NIST: NIST SP 800-53 (v3): PE-16
NIST: NIST SP 800-53 Revision 4 (v4): PE-16
NIST: NIST SP 800-53A (v1): PE-16.1 (iii)

---

**CCI:** CCI-002974 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-08-29
**Definition:** The organization defines types of information system components to authorize, monitor, and control entering and exiting the facility and to maintain records.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): PE-16

---

**CCI:** CCI-000985 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization employs organization-defined security controls at alternate work sites.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): PE-17 a
NIST: NIST SP 800-53 Revision 4 (v4): PE-17 a
NIST: NIST SP 800-53A (v1): PE-17.1 (ii)

---

**CCI:** CCI-002975 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-08-29
**Definition:** The organization defines security controls to employ at alternate work sites.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): PE-17 a

---

**CCI:** CCI-000987 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization assesses as feasible, the effectiveness of security controls at alternate work sites.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): PE-17 b
NIST: NIST SP 800-53 Revision 4 (v4): PE-17 b
NIST: NIST SP 800-53A (v1): PE-17.1 (iii)

---

**CCI:** CCI-000988 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization provides a means for employees to communicate with information security personnel in case of security incidents or problems.
**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PE-17 c

NIST: NIST SP 800-53 Revision 4 (v4): PE-17 c

NIST: NIST SP 800-53A (v1): PE-17.1 (iv)

---

**CCI:** CCI-000989 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization positions information system components within the facility to minimize potential damage from organization-defined physical and environmental hazards.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PE-18

NIST: NIST SP 800-53 Revision 4 (v4): PE-18

NIST: NIST SP 800-53A (v1): PE-18.1 (i)

---

**CCI:** CCI-000991 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization positions information system components within the facility to minimize the opportunity for unauthorized access.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PE-18

NIST: NIST SP 800-53 Revision 4 (v4): PE-18

NIST: NIST SP 800-53A (v1): PE-18.1 (ii)

---

**CCI:** CCI-002976 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-08-29

**Definition:** The organization defines physical and environmental hazards that could cause potential damage to information system components within the facility.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PE-18

---

**CCI:** CCI-002977 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-08-29

**Definition:** The organization plans the location or site of the facility where the information system resides with regard to physical and environmental hazards.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PE-18 (1)

---

**CCI:** CCI-002978 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-08-29

**Definition:** The organization considers the physical and environmental hazards in its risk mitigation strategy for existing facilities.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PE-18 (1)

---

**CCI:** CCI-000993 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization protects the information system from information leakage due to electromagnetic signals emanations.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PE-19

NIST: NIST SP 800-53 Revision 4 (v4): PE-19

NIST: NIST SP 800-53A (v1): PE-19.1

---

**CCI:** CCI-000994 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization ensures that information system components, associated data communications, and networks are protected in accordance with national emissions and TEMPEST policies and procedures based on the security category or classification of the information.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PE-19 (1)

NIST: NIST SP 800-53 Revision 4 (v4): PE-19 (1)

NIST: NIST SP 800-53A (v1): PE-19 (1).1

---

**CCI:** CCI-002979 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-08-29

**Definition:** The organization employs organization-defined asset location technologies to track and monitor the location and movement of organization-defined assets within organization-defined controlled areas.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PE-20 a

---

**CCI:** CCI-002980 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-08-29

**Definition:** The organization defines asset location technologies to track and monitor the location and movement of organization-defined assets within organization-defined controlled areas.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PE-20 a

---

**CCI:** CCI-002981 **Status:** draft

**Contributor:** DISA FSO **Published** 2013-08-29

**Date:**

**Definition:** The organization defines the assets within the organization-defined controlled areas which are to be tracked and monitored for their location and movement.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PE-20 a

---

**CCI:** CCI-002982 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-08-29

**Definition:** The organization defines controlled areas where the location and movement of organization-defined assets are tracked and monitored.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PE-20 a

---

**CCI:** CCI-002983 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-08-29

**Definition:** The organization ensures that asset location technologies are employed in accordance with applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PE-20 b

---

**CCI:** CCI-000563 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization develops and documents a security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PL-1 a
NIST: NIST SP 800-53 Revision 4 (v4): PL-1 a 1
NIST: NIST SP 800-53A (v1): PL-1.1 (i) (ii)

---

**CCI:** CCI-000564 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization disseminates a security planning policy to organization-defined personnel or roles.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PL-1 a
NIST: NIST SP 800-53 Revision 4 (v4): PL-1 a 1
NIST: NIST SP 800-53A (v1): PL-1.1 (iii)

---

**CCI:** CCI-000566 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization develops and documents procedures to facilitate the implementation of the security planning policy and associated security planning controls.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PL-1 b

NIST: NIST SP 800-53 Revision 4 (v4): PL-1 a 2

NIST: NIST SP 800-53A (v1): PL-1.1 (iv) (v)

---

**CCI:** CCI-000567 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization disseminates security planning procedures to organization-defined personnel or roles.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PL-1 b

NIST: NIST SP 800-53 Revision 4 (v4): PL-1 a 2

NIST: NIST SP 800-53A (v1): PL-1.1 (vi)

---

**CCI:** CCI-003047 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-23

**Definition:** The organization defines the personnel or roles to whom a security planning policy is disseminated.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PL-1 a 1

---

**CCI:** CCI-003048 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-23

**Definition:** The organization defines the personnel or roles to whom the security planning procedures are disseminated.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PL-1 a 2

---

**CCI:** CCI-001636 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2010-05-12

**Definition:** The organization defines the frequency with which to review and update the current security planning policy.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PL-1

NIST: NIST SP 800-53 Revision 4 (v4): PL-1 b 1

NIST: NIST SP 800-53A (v1): PL-1.2 (i)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001637 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-12 |
| **Definition:** | The organization reviews and updates the current security planning policy in accordance with organization-defined frequency. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PL-1 b<br>NIST: NIST SP 800-53 Revision 4 (v4): PL-1 b 1<br>NIST: NIST SP 800-53A (v1): PL-1.2 (ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001638 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-12 |
| **Definition:** | The organization defines the frequency with which to review and update the current security planning procedures. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PL-1 b<br>NIST: NIST SP 800-53 Revision 4 (v4): PL-1 b 2<br>NIST: NIST SP 800-53A (v1): PL-1.2 (iii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000568 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization reviews and updates the current security planning procedures in accordance with organization-defined frequency. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PL-1 b<br>NIST: NIST SP 800-53 Revision 4 (v4): PL-1 b 2<br>NIST: NIST SP 800-53A (v1): PL-1.2 (iv) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000571 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization's security plan for the information system is reviewed and approved by the authorizing official or designated representative prior to plan implementation. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PL-2 a<br>NIST: NIST SP 800-53 Revision 4 (v4): PL-2 a 9<br>NIST: NIST SP 800-53A (v1): PL-2.1 (i) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003049 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-23 |
| **Definition:** | The organization develops a security plan for the information system. | | |

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PL-2 a

---

**CCI:** CCI-003050 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-23

**Definition:** The organization's security plan for the information system is consistent with the organization's enterprise architecture.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PL-2 a 1

---

**CCI:** CCI-003051 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-23

**Definition:** The organization's security plan for the information system explicitly defines the authorization boundary for the system.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PL-2 a 2

---

**CCI:** CCI-003052 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-23

**Definition:** The organization's security plan for the information system describes the operational context of the information system in terms of missions and business processes.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PL-2 a 3

---

**CCI:** CCI-003053 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-23

**Definition:** The organization's security plan for the information system provides the security categorization of the information system, including supporting rationale.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PL-2 a 4

---

**CCI:** CCI-003054 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-23

**Definition:** The organization's security plan for the information system describes the operational environment for the information system and relationships with, or connections to, other information systems.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PL-2 a 5

---

**CCI:** CCI-003055 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-23

**Definition:** The organization's security plan for the information system provides an overview of the security requirements for the system.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PL-2 a 6

---

**CCI:** CCI-003056 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-23

**Definition:** The organization's security plan for the information system identifies any relevant overlays, if applicable.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PL-2 a 7

---

**CCI:** CCI-003057 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-23

**Definition:** The organization's security plan for the information system describes the security controls in place or planned for meeting those requirements, including a rationale for the tailoring decisions.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PL-2 a 8

---

**CCI:** CCI-003058 **Status:** deprecated

**Contributor:** DISA FSO **Published Date:** 2013-09-23

**Definition:** The organization distributes copies of the security plan to organization-defined personnel or roles.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PL-2 b

---

**CCI:** CCI-003059 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-23

**Definition:** The organization distributes copies of the security plan to organization-defined personnel or roles.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PL-2 b

---

**CCI:** CCI-003060 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-23

**Definition:** The organization defines the personnel or roles to whom copies of the security plan are distributed.

| | | | |
|---|---|---|---|
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PL-2 b | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003061 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-23 |
| **Definition:** | The organization communicates subsequent changes to the security plan to organization-defined personnel or roles. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PL-2 b | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003062 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-23 |
| **Definition:** | The organization defines the personnel or roles to whom changes to the security plan are communicated. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PL-2 b | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000572 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization defines the frequency for reviewing the security plan for the information system. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PL-2 b<br>NIST: NIST SP 800-53 Revision 4 (v4): PL-2 c<br>NIST: NIST SP 800-53A (v1): PL-2.1 (ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000573 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization reviews the security plan for the information system in accordance with organization-defined frequency. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PL-2 b<br>NIST: NIST SP 800-53 Revision 4 (v4): PL-2 c<br>NIST: NIST SP 800-53A (v1): PL-2.1 (iii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000574 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments. | | |

| | |
|---|---|
| **Type:** | policy |
| **References:** | NIST: NIST SP 800-53 (v3): PL-2 c<br>NIST: NIST SP 800-53 Revision 4 (v4): PL-2 d<br>NIST: NIST SP 800-53A (v1): PL-2.1 (iv) |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003063 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-23 |
| **Definition:** | The organization protects the security plan from unauthorized disclosure. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PL-2 e | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003064 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-23 |
| **Definition:** | The organization protects the security plan from unauthorized modification. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PL-2 e | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003065 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-23 |
| **Definition:** | The organization plans and coordinates security-related activities affecting the information system with organization-defined individuals or groups before conducting such activities in order to reduce the impact on other organizational entities. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PL-2 (3) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003066 | **Status:** | deprecated |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-23 |
| **Definition:** | The organization defines the individuals or groups with whom security-related activities are planned and coordinated. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PL-2 (3) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003067 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-23 |
| **Definition:** | The organization defines the individuals or groups with whom security-related activities are planned and coordinated. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PL-2 (3) | | |

---

**CCI:** CCI-001639 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2010-05-12
**Definition:** The organization makes readily available to individuals requiring access to the information system the rules that describe their responsibilities and expected behavior with regard to information and information system usage.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): PL-4 a
NIST: NIST SP 800-53 Revision 4 (v4): PL-4 a
NIST: NIST SP 800-53A (v1): PL-4.1 (ii)

---

**CCI:** CCI-000592 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization establishes the rules describing the responsibilities and expected behavior, with regard to information and information system usage, for individuals requiring access to the information system.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): PL-4 a
NIST: NIST SP 800-53 Revision 4 (v4): PL-4 a
NIST: NIST SP 800-53A (v1): PL-4.1 (i)

---

**CCI:** CCI-000593 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization receives a signed acknowledgment from individuals requiring access to the information system, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): PL-4 b
NIST: NIST SP 800-53 Revision 4 (v4): PL-4 b
NIST: NIST SP 800-53A (v1): PL-4.1 (iii)

---

**CCI:** CCI-003068 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-09-23
**Definition:** The organization reviews and updates the rules of behavior in accordance with organization-defined frequency.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): PL-4 c

---

**CCI:** CCI-003069 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-09-23
**Definition:** The organization defines the frequency with which to review and update the rules of

behavior.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PL-4 c

---

**CCI:** CCI-003070 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-23

**Definition:** The organization requires individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised/updated.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PL-4 d

---

**CCI:** CCI-000594 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization includes in the rules of behavior explicit restrictions on the use of social media/networking sites.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PL-4 (1)
NIST: NIST SP 800-53 Revision 4 (v4): PL-4 (1)
NIST: NIST SP 800-53A (v1): PL-4 (1).1

---

**CCI:** CCI-000595 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization includes in the rules of behavior explicit restrictions on posting organizational information on public websites.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PL-4 (1)
NIST: NIST SP 800-53 Revision 4 (v4): PL-4 (1)
NIST: NIST SP 800-53A (v1): PL-4 (1).1

---

**CCI:** CCI-003071 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-23

**Definition:** The organization develops a security Concept of Operations (CONOPS) for the information system containing, at a minimum, how the organization intends to operate the system from the perspective of information security.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PL-7 a

---

**CCI:** CCI-000577 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization defines the frequency with which to review and update the security CONOPS.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PL-2 (1) (b)
NIST: NIST SP 800-53 Revision 4 (v4): PL-7 b
NIST: NIST SP 800-53A (v1): PL-2 (1).1 (iii)

---

**CCI:** CCI-000578 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization reviews and updates the security CONOPS in accordance with organization-defined frequency.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PL-2 (1) (b)
NIST: NIST SP 800-53 Revision 4 (v4): PL-7 b
NIST: NIST SP 800-53A (v1): PL-2 (1).1 (iv)

---

**CCI:** CCI-003072 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-23

**Definition:** The organization develops an information security architecture for the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PL-8 a

---

**CCI:** CCI-003073 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-23

**Definition:** The organization's information security architecture for the information system describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PL-8 a 1

---

**CCI:** CCI-003074 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-23

**Definition:** The organization's information security architecture for the information system describes how the information security architecture is integrated into and supports the enterprise architecture.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PL-8 a 2

---

**CCI:** CCI-003075 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-23

**Definition:** The organization's information security architecture for the information system describes any information security assumptions about, and dependencies on, external services.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PL-8 a 3

---

**CCI:** CCI-003076 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-23

**Definition:** The organization reviews and updates the information security architecture in accordance with organization-defined frequency to reflect updates in the enterprise architecture.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PL-8 b

---

**CCI:** CCI-003077 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-23

**Definition:** The organization defines the frequency with which to review and update the information system architecture.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PL-8 b

---

**CCI:** CCI-003078 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-23

**Definition:** The organization ensures that planned information security architecture changes are reflected in the security plan.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PL-8 c

---

**CCI:** CCI-003079 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-23

**Definition:** The organization ensures that planned information security architecture changes are reflected in the security Concept of Operations (CONOPS).

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PL-8 c

---

**CCI:** CCI-003080 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-23

**Definition:** The organization ensures that planned information security architecture changes are reflected in organizational procurements/acquisitions.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PL-8 c

---

**CCI:** CCI-003081 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-23

**Definition:** The organization designs its security architecture using a defense-in-depth approach that allocates organization-defined security safeguards to organization-defined locations.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PL-8 (1) (a)

---

**CCI:** CCI-003082 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-23

**Definition:** The organization designs its security architecture using a defense-in-depth approach that allocates organization-defined security safeguards to organization-defined architectural layers.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PL-8 (1) (a)

---

**CCI:** CCI-003083 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-23

**Definition:** The organization defines the security safeguards to be allocated to organization-defined locations.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PL-8 (1) (a)

---

**CCI:** CCI-003084 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-23

**Definition:** The organization defines the security safeguards to be allocated to organization-defined architectural layers.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PL-8 (1) (a)

---

**CCI:** CCI-003085 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-23

**Definition:** The organization defines the locations to which it allocates organization-defined security safeguards in the security architecture.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PL-8 (1) (a)

---

**CCI:** CCI-003086 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-23

**Definition:** The organization defines the architectural layers to which it allocates organization-defined

| | | | |
|---|---|---|---|
| | security safeguards in the security architecture. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PL-8 (1) (a) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003087 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-23 |
| **Definition:** | The organization designs its security architecture using a defense-in-depth approach that ensures that the allocated security safeguards operate in a coordinated and mutually reinforcing manner. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PL-8 (1) (b) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003088 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-23 |
| **Definition:** | The organization requires that organization-defined security safeguards allocated to organization-defined locations and architectural layers be obtained from different suppliers. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PL-8 (2) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003117 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-23 |
| **Definition:** | The organization centrally manages organization-defined security controls and related processes. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PL-9 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003118 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-23 |
| **Definition:** | The organization defines security controls and related processes to be centrally managed. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PL-9 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001680 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-06-09 |
| **Definition:** | The organization develops an organization-wide information security program plan that includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PM-1 a<br>NIST: NIST SP 800-53 Revision 4 (v4): PM-1 a 2 | | |

NIST: NIST SP 800-53A (v1): PM-1.1 (i)

---

**CCI:** CCI-000073 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-11-03

**Definition:** The organization develops an organization-wide information security program plan that provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PM-1 a

NIST: NIST SP 800-53 Revision 4 (v4): PM-1 a 1

NIST: NIST SP 800-53A (v1): PM-1.1 (i)

---

**CCI:** CCI-000074 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-11-03

**Definition:** The organization develops an organization-wide information security program plan that is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PM-1 a

NIST: NIST SP 800-53 Revision 4 (v4): PM-1 a 4

NIST: NIST SP 800-53A (v1): PM-1.1 (i)

---

**CCI:** CCI-002984 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-08-29

**Definition:** The organization develops an organization-wide information security program plan that reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical).

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PM-1 a 3

---

**CCI:** CCI-002985 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-08-29

**Definition:** The organization disseminates an organization-wide information security program plan that provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PM-1 a 1

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002986 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-08-29 |
| **Definition:** | The organization disseminates an organization-wide information security program plan that includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PM-1 a 2 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002987 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-08-29 |
| **Definition:** | The organization disseminates an organization-wide information security program plan that reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical). | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PM-1 a 3 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002988 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-08-29 |
| **Definition:** | The organization disseminates an organization-wide information security program plan that is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PM-1 a 4 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000075 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-11-03 |
| **Definition:** | The organization reviews the organization-wide information security program plan on an organization-defined frequency. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PM-1 b<br>NIST: NIST SP 800-53 Revision 4 (v4): PM-1 b<br>NIST: NIST SP 800-53A (v1): PM-1.1 (iii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000076 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-11-03 |
| **Definition:** | The organization defines the frequency with which to review the organization-wide information security program plan. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PM-1 b | | |

| | | | |
|---|---|---|---|
| | NIST: NIST SP 800-53 Revision 4 (v4): PM-1 b<br>NIST: NIST SP 800-53A (v1): PM-1.1 (ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000077 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-11-03 |
| **Definition:** | The organization updates the plan to address organizational changes and problems identified during plan implementation or security control assessments. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PM-1 c<br>NIST: NIST SP 800-53 Revision 4 (v4): PM-1 c<br>NIST: NIST SP 800-53A (v1): PM-1.1 (iv) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002989 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-08-29 |
| **Definition:** | The organization protects the information security program plan from unauthorized disclosure. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PM-1 d | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002990 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-08-29 |
| **Definition:** | The organization protects the information security program plan from unauthorized modification. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PM-1 d | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000078 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-11-03 |
| **Definition:** | The organization appoints a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PM-2<br>NIST: NIST SP 800-53 Revision 4 (v4): PM-2<br>NIST: NIST SP 800-53A (v1): PM-2.1 (i and ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000080 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-11-03 |
| **Definition:** | The organization ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all | | |

exceptions to this requirement.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PM-3 a
NIST: NIST SP 800-53 Revision 4 (v4): PM-3 a
NIST: NIST SP 800-53A (v1): PM-3.1 (i and ii)

---

**CCI:** CCI-000081 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-11-03

**Definition:** The organization employs a business case/Exhibit 300/Exhibit 53 to record the resources required.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PM-3 b
NIST: NIST SP 800-53 Revision 4 (v4): PM-3 b
NIST: NIST SP 800-53A (v1): PM-3.1 (iii)

---

**CCI:** CCI-000141 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-11-03

**Definition:** The organization ensures that information security resources are available for expenditure as planned.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PM-3 c
NIST: NIST SP 800-53 Revision 4 (v4): PM-3 c
NIST: NIST SP 800-53A (v1): PM-3.1 (iv)

---

**CCI:** CCI-000142 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-11-03

**Definition:** The organization implements a process for ensuring that plans of action and milestones for the security program and the associated organizational information systems are maintained.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PM-4
NIST: NIST SP 800-53 Revision 4 (v4): PM-4 a 1
NIST: NIST SP 800-53A (v1): PM-4.1 (i)

---

**CCI:** CCI-000170 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-11-03

**Definition:** The organization implements a process for ensuring that plans of action and milestones for the security program and associated organizational information systems document the remedial information security actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation.

**Type:** policy

| | | | |
|---|---|---|---|
| **References:** | NIST: NIST SP 800-53 (v3): PM-4<br>NIST: NIST SP 800-53 Revision 4 (v4): PM-4 a 2<br>NIST: NIST SP 800-53A (v1): PM-4.1 (ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002991 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-08-29 |
| **Definition:** | The organization implements a process for ensuring that plans of action and milestones for the security program and associated organizational information systems are developed. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PM-4 a 1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002992 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-08-29 |
| **Definition:** | The organization implements a process for ensuring that plans of action and milestones for the security program and associated organizational information systems are reported in accordance with OMB FISMA reporting requirements. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PM-4 a 3 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002993 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-08-29 |
| **Definition:** | The organization reviews plans of action and milestones for the security program and associated organization information systems for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PM-4 b | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000207 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-11-03 |
| **Definition:** | The organization develops and maintains an inventory of its information systems. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PM-5<br>NIST: NIST SP 800-53 Revision 4 (v4): PM-5<br>NIST: NIST SP 800-53A (v1): PM-5.1 (i and ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000209 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-11-03 |
| **Definition:** | The organization develops the results of information security measures of performance. | | |
| **Type:** | policy | | |

**References:** NIST: NIST SP 800-53 (v3): PM-6
NIST: NIST SP 800-53 Revision 4 (v4): PM-6
NIST: NIST SP 800-53A (v1): PM-6.1 (i)

---

**CCI:** CCI-000210 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-11-03
**Definition:** The organization monitors the results of information security measures of performance.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): PM-6
NIST: NIST SP 800-53 Revision 4 (v4): PM-6
NIST: NIST SP 800-53A (v1): PM-6.1 (ii)

---

**CCI:** CCI-000211 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-11-03
**Definition:** The organization reports on the results of information security measures of performance.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): PM-6
NIST: NIST SP 800-53 Revision 4 (v4): PM-6
NIST: NIST SP 800-53A (v1): PM-6.1 (iii)

---

**CCI:** CCI-000212 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-11-03
**Definition:** The organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): PM-7
NIST: NIST SP 800-53 Revision 4 (v4): PM-7
NIST: NIST SP 800-53A (v1): PM-7.1

---

**CCI:** CCI-001640 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2010-05-12
**Definition:** The organization updates the critical infrastructure and key resources protection plan that addresses information security issues.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): PM-8
NIST: NIST SP 800-53 Revision 4 (v4): PM-8
NIST: NIST SP 800-53A (v1): PM-8.1 (ii)

---

**CCI:** CCI-000216 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-11-03

**Definition:** The organization develops and documents a critical infrastructure and key resource protection plan that addresses information security issues.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PM-8
NIST: NIST SP 800-53 Revision 4 (v4): PM-8
NIST: NIST SP 800-53A (v1): PM-8.1 (I and iii)

---

**CCI:** CCI-000227 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-11-03

**Definition:** The organization develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PM-9 a
NIST: NIST SP 800-53 Revision 4 (v4): PM-9 a
NIST: NIST SP 800-53A (v1): PM-9.1 (i)

---

**CCI:** CCI-000228 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-11-03

**Definition:** The organization implements a comprehensive strategy to manage risk to organization operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems consistently across the organization.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PM-9 b
NIST: NIST SP 800-53 Revision 4 (v4): PM-9 b
NIST: NIST SP 800-53A (v1): PM-9.1 (ii)

---

**CCI:** CCI-002994 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-08-29

**Definition:** The organization reviews and updates the risk management strategy in accordance with organization-defined frequency or as required, to address organizational changes.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PM-9 c

---

**CCI:** CCI-002995 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-08-29

**Definition:** The organization defines the frequency with which to review and update the risk management strategy to address organizational changes.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PM-9 c

---

**CCI:** CCI-000229 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-11-03

**Definition:** The organization documents the security state of organizational information systems and the environments in which those systems operate through security authorization processes.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PM-10 a

NIST: NIST SP 800-53 Revision 4 (v4): PM-10 a

NIST: NIST SP 800-53A (v1): PM-10.1 (i)

---

**CCI:** CCI-000230 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-11-03

**Definition:** The organization tracks the security state of organizational information systems and the environments in which those systems operate through security authorization processes.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PM-10 a

NIST: NIST SP 800-53 Revision 4 (v4): PM-10 a

NIST: NIST SP 800-53A (v1): PM-10.1 (i)

---

**CCI:** CCI-000231 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-11-03

**Definition:** The organization reports the security state of organizational information systems and the environments in which those systems operate through security authorization processes.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PM-10 a

NIST: NIST SP 800-53 Revision 4 (v4): PM-10 a

NIST: NIST SP 800-53A (v1): PM-10.1 (i)

---

**CCI:** CCI-000233 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-11-03

**Definition:** The organization designates individuals to fulfill specific roles and responsibilities within the organizational risk management process.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PM-10 b

NIST: NIST SP 800-53 Revision 4 (v4): PM-10 b

NIST: NIST SP 800-53A (v1): PM-10.1 (ii)

---

**CCI:** CCI-000234 **Status:** draft

**Contributor:** DISA FSO **Published** 2009-11-03

**Date:**

**Definition:** The organization fully integrates the security authorization processes into an organization-wide risk management program.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PM-10 c
NIST: NIST SP 800-53 Revision 4 (v4): PM-10 c
NIST: NIST SP 800-53A (v1): PM-10.1 (iii)

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-000235 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-11-04 |

**Definition:** The organization defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PM-11 a
NIST: NIST SP 800-53 Revision 4 (v4): PM-11 a
NIST: NIST SP 800-53A (v1): PM-11.1 (i)

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-000236 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-11-04 |

**Definition:** The organization determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until an achievable set of protection needs are obtained.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PM-11 b
NIST: NIST SP 800-53 Revision 4 (v4): PM-11 b
NIST: NIST SP 800-53A (v1): PM-11.1 (ii)

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-002996 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-08-29 |

**Definition:** The organization implements an insider threat program that includes a cross-discipline insider threat incident handling team.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PM-12

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-002997 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-08-29 |

**Definition:** The organization establishes an information security workforce development and improvement program.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PM-13

---

**CCI:** CCI-002998 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-08-29

**Definition:** The organization implements a process for ensuring that organizational plans for conducting security testing activities associated with organizational information systems are developed.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PM-14 a 1

---

**CCI:** CCI-002999 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-08-29

**Definition:** The organization implements a process for ensuring that organizational plans for conducting security testing activities associated with organizational information systems are maintained.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PM-14 a 1

---

**CCI:** CCI-003000 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-08-29

**Definition:** The organization implements a process for ensuring that organizational plans for conducting security training activities associated with organizational information systems are developed.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PM-14 a 1

---

**CCI:** CCI-003001 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-08-29

**Definition:** The organization implements a process for ensuring that organizational plans for conducting security training activities associated with organizational information systems are maintained.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PM-14 a 1

---

**CCI:** CCI-003002 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-08-29

**Definition:** The organization implements a process for ensuring that organizational plans for conducting security monitoring activities associated with organizational information systems are developed.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PM-14 a 1

---

**CCI:** CCI-003003 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-08-29

**Definition:** The organization implements a process for ensuring that organizational plans for conducting security monitoring activities associated with organizational information systems are maintained.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PM-14 a 1

---

**CCI:** CCI-003004 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-08-29

**Definition:** The organization implements a process for ensuring that organizational plans for conducting security testing associated with organizational information systems continue to be executed in a timely manner.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PM-14 a 2

---

**CCI:** CCI-003005 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-08-29

**Definition:** The organization implements a process for ensuring that organizational plans for conducting security training associated with organizational information systems continue to be executed in a timely manner.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PM-14 a 2

---

**CCI:** CCI-003006 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-08-29

**Definition:** The organization implements a process for ensuring that organizational plans for conducting security monitoring activities associated with organizational information systems continue to be executed in a timely manner.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PM-14 a 2

---

**CCI:** CCI-003007 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-08-29

**Definition:** The organization reviews testing plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PM-14 b

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003008 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-08-29 |
| **Definition:** | The organization reviews training plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PM-14 b | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003009 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-08-29 |
| **Definition:** | The organization reviews monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PM-14 b | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003010 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-08-29 |
| **Definition:** | The organization establishes and institutionalizes contact with selected groups and associations within the security community to facilitate ongoing security education and training for organizational personnel. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PM-15 a | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003011 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-08-29 |
| **Definition:** | The organization establishes and institutionalizes contact with selected groups and associations within the security community to maintain currency with recommended security practices, techniques, and technologies. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PM-15 b | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003012 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-08-29 |
| **Definition:** | The organization establishes and institutionalizes contact with selected groups and associations within the security community to share current security-related information including threats, vulnerabilities, and incidents. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PM-15 c | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003013 | **Status:** | draft |

| | | | |
|---|---|---|---|
| **Contributor:** | DISA FSO | **Published Date:** | 2013-08-29 |
| **Definition:** | The organization implements a threat awareness program that includes a cross-organization information-sharing capability. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PM-16 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001504 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-11-02 |
| **Definition:** | The organization develops and documents a personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PS-1 a<br>NIST: NIST SP 800-53 Revision 4 (v4): PS-1 a 1<br>NIST: NIST SP 800-53A (v1): PS-1.1 (i) (ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001505 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-11-02 |
| **Definition:** | The organization disseminates a personnel security policy to organization-defined personnel or roles. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PS-1 a<br>NIST: NIST SP 800-53 Revision 4 (v4): PS-1 a 1<br>NIST: NIST SP 800-53A (v1): PS-1.1 (iii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001509 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-11-02 |
| **Definition:** | The organization develops and documents procedures to facilitate the implementation of the personnel security policy and associated personnel security controls. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PS-1 b<br>NIST: NIST SP 800-53 Revision 4 (v4): PS-1 a 2<br>NIST: NIST SP 800-53A (v1): PS-1.1 (iv) (v) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001510 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-11-02 |
| **Definition:** | The organization disseminates personnel security procedures to organization-defined personnel or roles. | | |
| **Type:** | policy | | |

**References:** NIST: NIST SP 800-53 (v3): PS-1 b
NIST: NIST SP 800-53 Revision 4 (v4): PS-1 a 2
NIST: NIST SP 800-53A (v1): PS-1.1 (vi)

---

**CCI:** CCI-003017 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-09-12
**Definition:** The organization defines the personnel or roles to whom a personnel security policy is disseminated.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): PS-1 a 1

---

**CCI:** CCI-003018 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-09-12
**Definition:** The organization defines the personnel or roles to whom the personnel security procedures are disseminated.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): PS-1 a 2

---

**CCI:** CCI-001506 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-11-02
**Definition:** The organization reviews and updates the current personnel security policy in accordance with organization-defined frequency.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): PS-1 a
NIST: NIST SP 800-53 Revision 4 (v4): PS-1 b 2
NIST: NIST SP 800-53A (v1): PS-1.2 (ii)

---

**CCI:** CCI-001507 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-11-02
**Definition:** The organization defines the frequency with which to review and update the current personnel security policy.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): PS-1 a
NIST: NIST SP 800-53 Revision 4 (v4): PS-1 b 1
NIST: NIST SP 800-53A (v1): PS-1.2 (i)

---

**CCI:** CCI-001508 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-11-02
**Definition:** The organization defines the frequency with which to review and update the current

personnel security procedures.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PS-1 b
NIST: NIST SP 800-53 Revision 4 (v4): PS-1 b 2
NIST: NIST SP 800-53A (v1): PS-1.2 (iii)

---

**CCI:** CCI-001511 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-11-02

**Definition:** The organization reviews and updates the current personnel security procedures in accordance with organization-defined frequency.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PS-1 b
NIST: NIST SP 800-53 Revision 4 (v4): PS-1 b 2
NIST: NIST SP 800-53A (v1): PS-1.2 (iv)

---

**CCI:** CCI-001512 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-11-02

**Definition:** The organization assigns a risk designation to all organizational positions.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PS-2 a
NIST: NIST SP 800-53 Revision 4 (v4): PS-2 a
NIST: NIST SP 800-53A (v1): PS-2.1 (i)

---

**CCI:** CCI-001513 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-11-02

**Definition:** The organization establishes screening criteria for individuals filling organizational positions.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PS-2 b
NIST: NIST SP 800-53 Revision 4 (v4): PS-2 b
NIST: NIST SP 800-53A (v1): PS-2.1 (ii)

---

**CCI:** CCI-001514 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-11-02

**Definition:** The organization reviews and updates position risk designations in accordance with organization-defined frequency.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PS-2 c
NIST: NIST SP 800-53 Revision 4 (v4): PS-2 c
NIST: NIST SP 800-53A (v1): PS-2.1 (iv)

---

**CCI:** CCI-001515 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-11-02

**Definition:** The organization defines the frequency with which to review and update position risk designations.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PS-2 c

NIST: NIST SP 800-53 Revision 4 (v4): PS-2 c

NIST: NIST SP 800-53A (v1): PS-2.1 (iii)

---

**CCI:** CCI-001516 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-11-02

**Definition:** The organization screens individuals prior to authorizing access to the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PS-3 a

NIST: NIST SP 800-53 Revision 4 (v4): PS-3 a

NIST: NIST SP 800-53A (v1): PS-3.1 (i)

---

**CCI:** CCI-001517 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-11-02

**Definition:** The organization rescreens individuals with authorized access to the information system according to organization-defined conditions requiring rescreening, and where rescreening is so indicated, on the organization-defined frequency of such rescreening.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PS-3 b

NIST: NIST SP 800-53 Revision 4 (v4): PS-3 b

NIST: NIST SP 800-53A (v1): PS-3.1 (iii)

---

**CCI:** CCI-001518 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-11-02

**Definition:** The organization defines the conditions requiring rescreening of individuals with authorized access to the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PS-3 b

NIST: NIST SP 800-53 Revision 4 (v4): PS-3 b

NIST: NIST SP 800-53A (v1): PS-3.1 (ii)

---

**CCI:** CCI-001519 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-11-02

**Definition:** The organization defines the frequency for rescreening individuals with authorized access to the information system when organization-defined conditions requiring rescreening are met.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PS-3 b
NIST: NIST SP 800-53 Revision 4 (v4): PS-3 b
NIST: NIST SP 800-53A (v1): PS-3.1 (ii)

---

**CCI:** CCI-001520 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-11-02

**Definition:** The organization ensures that individuals accessing an information system processing, storing, or transmitting classified information are cleared and indoctrinated to the highest classification level of the information to which they have access on the system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PS-3 (1)
NIST: NIST SP 800-53 Revision 4 (v4): PS-3 (1)
NIST: NIST SP 800-53A (v1): PS-3 (1).1 (i) (ii)

---

**CCI:** CCI-001521 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-11-02

**Definition:** The organization ensures that individuals accessing an information system processing, storing, or transmitting types of classified information which require formal indoctrination, are formally indoctrinated for all of the relevant types of information to which they have access on the system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PS-3 (2)
NIST: NIST SP 800-53 Revision 4 (v4): PS-3 (2)
NIST: NIST SP 800-53A (v1): PS-3 (2).1

---

**CCI:** CCI-003019 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-12

**Definition:** The organization ensures that individuals accessing an information system processing, storing, or transmitting information requiring special protection have valid access authorizations that are demonstrated by assigned official government duties.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PS-3 (3) (a)

---

**CCI:** CCI-003020 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-12

**Definition:** The organization ensures that individuals accessing an information system processing, storing, or transmitting information requiring special protection satisfy organization-defined additional personnel screening criteria.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PS-3 (3) (b)

---

**CCI:** CCI-003021 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-12

**Definition:** The organization defines additional personnel screening criteria that individuals accessing an information system processing, storing, or transmitting information requiring protection must satisfy.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PS-3 (3) (b)

---

**CCI:** CCI-001522 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-11-02

**Definition:** The organization, upon termination of individual employment, disables information system access within an organization-defined time period.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PS-4 a
NIST: NIST SP 800-53 Revision 4 (v4): PS-4 a
NIST: NIST SP 800-53A (v1): PS-4.1 (i)

---

**CCI:** CCI-003022 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-12

**Definition:** The organization defines the time period within which to disable information system access upon termination of individual employment.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PS-4 a

---

**CCI:** CCI-003023 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-12

**Definition:** The organization, upon termination of individual employment, terminates/revokes any authenticators/credentials associated with the individual.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PS-4 b

---

**CCI:** CCI-001523 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-11-02

**Definition:** The organization, upon termination of individual employment, conducts exit interviews that include a discussion of organization-defined information security topics.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PS-4 b

NIST: NIST SP 800-53 Revision 4 (v4): PS-4 c
NIST: NIST SP 800-53A (v1): PS-4.1 (ii)

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003024 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-12 |
| **Definition:** | The organization defines information security topics to be discussed while conducting exit interviews. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PS-4 c | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001524 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-11-02 |
| **Definition:** | The organization, upon termination of individual employment, retrieves all security-related organizational information system-related property. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PS-4 c<br>NIST: NIST SP 800-53 Revision 4 (v4): PS-4 d<br>NIST: NIST SP 800-53A (v1): PS-4.1 (iii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001525 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-11-02 |
| **Definition:** | The organization, upon termination of individual employment, retains access to organizational information formerly controlled by the terminated individual. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PS-4 d<br>NIST: NIST SP 800-53 Revision 4 (v4): PS-4 e<br>NIST: NIST SP 800-53A (v1): PS-4.1 (iv) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001526 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-11-02 |
| **Definition:** | The organization, upon termination of individual employment, retains access to organizational information systems formerly controlled by the terminated individual. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PS-4 d<br>NIST: NIST SP 800-53 Revision 4 (v4): PS-4 e<br>NIST: NIST SP 800-53A (v1): PS-4.1 (iv) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003016 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-12 |

**Definition:** The organization, upon termination of individual employment, notifies organization-defined personnel or roles within an organization-defined time period.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PS-4 f

---

**CCI:** CCI-003025 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-12

**Definition:** The organization defines personnel or roles to notify upon termination of individual employment.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PS-4 f

---

**CCI:** CCI-003026 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-12

**Definition:** The organization defines the time period within which to notify organization-defined personnel or roles upon termination of individual employment.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PS-4 f

---

**CCI:** CCI-003027 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-12

**Definition:** The organization notifies terminated individuals of applicable, legally binding post-employment requirements for the protection of organizational information.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PS-4 (1) (a)

---

**CCI:** CCI-003028 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-12

**Definition:** The organization requires terminated individuals to sign an acknowledgment of post-employment requirements as part of the organizational termination process.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PS-4 (1) (b)

---

**CCI:** CCI-003029 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-12

**Definition:** The organization employs automated mechanisms to notify organization-defined personnel or roles upon termination of an individual.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PS-4 (2)

---

**CCI:** CCI-003030 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-12

**Definition:** The organization defines the personnel or roles to be notified by automated mechanism upon termination of an individual.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PS-4 (2)

---

**CCI:** CCI-001527 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-11-03

**Definition:** The organization reviews and confirms the ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PS-5

NIST: NIST SP 800-53 Revision 4 (v4): PS-5 a

NIST: NIST SP 800-53A (v1): PS-5.1 (i)

---

**CCI:** CCI-001528 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-11-03

**Definition:** The organization initiates organization-defined transfer or reassignment actions within an organization-defined time period following the formal personnel transfer action.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PS-5

NIST: NIST SP 800-53 Revision 4 (v4): PS-5 b

NIST: NIST SP 800-53A (v1): PS-5.1 (iii)

---

**CCI:** CCI-001529 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-11-03

**Definition:** The organization defines transfer or reassignment actions to initiate within an organization-defined time period following the formal personnel transfer action.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PS-5

NIST: NIST SP 800-53 Revision 4 (v4): PS-5 b

NIST: NIST SP 800-53A (v1): PS-5.1 (ii)

---

**CCI:** CCI-001530 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-11-03

**Definition:** The organization defines the time period within which the organization initiates organization-defined transfer or reassignment actions following the formal personnel transfer action.

| | | | |
|---|---|---|---|
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PS-5<br>NIST: NIST SP 800-53 Revision 4 (v4): PS-5 b<br>NIST: NIST SP 800-53A (v1): PS-5.1 (ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003031 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-12 |
| **Definition:** | The organization modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PS-5 c | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003032 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-12 |
| **Definition:** | The organization notifies organization-defined personnel or roles within an organization-defined time period when individuals are transferred or reassigned to other positions within the organization. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PS-5 d | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003033 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-12 |
| **Definition:** | The organization defines personnel or roles to be notified when individuals are transferred or reassigned to other positions within the organization. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PS-5 d | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003034 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-12 |
| **Definition:** | The organization defines the time period within which organization-defined personnel or roles are to be notified when individuals are transferred or reassigned to other positions within the organization. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): PS-5 d | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003035 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-12 |
| **Definition:** | The organization develops and documents access agreements for organizational information systems. | | |
| **Type:** | policy | | |

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PS-6 a

---

**CCI:** CCI-001532 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-11-03

**Definition:** The organization reviews and updates access agreements for organizational information systems in accordance with organization-defined frequency.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PS-6 b
NIST: NIST SP 800-53 Revision 4 (v4): PS-6 b
NIST: NIST SP 800-53A (v1): PS-6.1 (iv)

---

**CCI:** CCI-001533 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-11-03

**Definition:** The organization defines the frequency with which to review and update access agreements for organizational information systems.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PS-6 b
NIST: NIST SP 800-53 Revision 4 (v4): PS-6 b
NIST: NIST SP 800-53A (v1): PS-6.1 (iii)

---

**CCI:** CCI-001531 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-11-03

**Definition:** The organization ensures that individuals requiring access to organizational information and information systems sign appropriate access agreements prior to being granted access.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PS-6 a
NIST: NIST SP 800-53 Revision 4 (v4): PS-6 c 1
NIST: NIST SP 800-53A (v1): PS-6.1 (i) (ii)

---

**CCI:** CCI-003036 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-12

**Definition:** The organization ensures that individuals requiring access to organizational information and information systems re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or in accordance with organization-defined frequency.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PS-6 c 2

---

**CCI:** CCI-003037 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-12

**Definition:** The organization defines the frequency for individuals requiring access to organization information and information systems to re-sign access agreements.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PS-6 c 2

---

**CCI:** CCI-001536 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-11-03

**Definition:** The organization ensures that access to classified information requiring special protection is granted only to individuals who have a valid access authorization that is demonstrated by assigned official government duties.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PS-6 (2) (a)
NIST: NIST SP 800-53 Revision 4 (v4): PS-6 (2) (a)
NIST: NIST SP 800-53A (v1): PS-6 (2).1

---

**CCI:** CCI-001537 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-11-03

**Definition:** The organization ensures that access to classified information requiring special protection is granted only to individuals who satisfy associated personnel security criteria.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PS-6 (2) (b)
NIST: NIST SP 800-53 Revision 4 (v4): PS-6 (2) (b)
NIST: NIST SP 800-53A (v1): PS-6 (2).1

---

**CCI:** CCI-001538 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-11-03

**Definition:** The organization ensures that access to classified information requiring special protection is granted only to individuals who have read, understood, and signed a nondisclosure agreement.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PS-6 (2) (c)
NIST: NIST SP 800-53 Revision 4 (v4): PS-6 (2) (c)
NIST: NIST SP 800-53A (v1): PS-6 (2).1

---

**CCI:** CCI-003038 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-12

**Definition:** The organization notifies individuals of applicable, legally binding post-employment requirements for protection of organizational information.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PS-6 (3) (a)

---

**CCI:** CCI-003039 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-12

**Definition:** The organization requires individuals to sign an acknowledgement of legally binding post-employment requirements for protection of organizational information, if applicable, as part of granting initial access to covered information.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PS-6 (3) (b)

---

**CCI:** CCI-001539 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-11-03

**Definition:** The organization establishes personnel security requirements including security roles and responsibilities for third-party providers.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PS-7 a
NIST: NIST SP 800-53 Revision 4 (v4): PS-7 a
NIST: NIST SP 800-53A (v1): PS-7.1 (i)

---

**CCI:** CCI-003040 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-12

**Definition:** The organization requires third-party providers to comply with personnel security policies and procedures established by the organization.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PS-7 b

---

**CCI:** CCI-001540 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-11-03

**Definition:** The organization documents personnel security requirements for third-party providers.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PS-7 b
NIST: NIST SP 800-53 Revision 4 (v4): PS-7 c
NIST: NIST SP 800-53A (v1): PS-7.1 (ii)

---

**CCI:** CCI-003041 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-12

**Definition:** The organization requires third-party providers to notify organization-defined personnel or roles of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within an organization-defined time period.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PS-7 d

---

**CCI:** CCI-003042 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-12

**Definition:** The organization defines personnel or roles whom third-party providers are to notify when third-party personnel who possess organizational credentials and /or badges or who have information system privileges are transferred or terminated.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PS-7 d

---

**CCI:** CCI-003043 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-12

**Definition:** The organization defines the time period for third-party providers to notify organization-defined personnel or roles when third-party personnel who possess organizational credentials and /or badges or who have information system privileges are transferred or terminated.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PS-7 d

---

**CCI:** CCI-001541 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-11-03

**Definition:** The organization monitors third-party provider compliance with personnel security requirements.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PS-7 c
NIST: NIST SP 800-53 Revision 4 (v4): PS-7 e
NIST: NIST SP 800-53A (v1): PS-7.1 (iii)

---

**CCI:** CCI-001542 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-11-03

**Definition:** The organization employs a formal sanctions process for individuals failing to comply with established information security policies and procedures.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PS-8
NIST: NIST SP 800-53 Revision 4 (v4): PS-8 a
NIST: NIST SP 800-53A (v1): PS-8.1

---

**CCI:** CCI-003044 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-12

**Definition:** The organization notifies organization-defined personnel or roles within an organization-defined time period when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PS-8 b

---

**CCI:** CCI-003045 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-12

**Definition:** The organization defines personnel or roles who are to be notified when a formal employee sanctions process is initiated.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PS-8 b

---

**CCI:** CCI-003046 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-12

**Definition:** The organization defines the time period within which to notify organization-defined personnel or roles when a formal employee sanctions process is initiated.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): PS-8 b

---

**CCI:** CCI-001037 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization develops and documents a risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): RA-1 a
NIST: NIST SP 800-53 Revision 4 (v4): RA-1 a 1
NIST: NIST SP 800-53A (v1): RA-1.1 (i) (ii)

---

**CCI:** CCI-001038 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization disseminates a risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance to organization-defined personnel or roles.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): RA-1 a
NIST: NIST SP 800-53 Revision 4 (v4): RA-1 a 1
NIST: NIST SP 800-53A (v1): RA-1.1 (iii)

---

**CCI:** CCI-001041 **Status:** draft

**Contributor:** DISA FSO **Published** 2009-09-21

| | | | |
|---|---|---|---|
| | | **Date:** | |
| **Definition:** | The organization develops and documents procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): RA-1 b<br>NIST: NIST SP 800-53 Revision 4 (v4): RA-1 a 2<br>NIST: NIST SP 800-53A (v1): RA-1.1 (iv) (v) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001042 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization disseminates risk assessment procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls to organization-defined personnel or roles. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): RA-1 b<br>NIST: NIST SP 800-53 Revision 4 (v4): RA-1 a 2<br>NIST: NIST SP 800-53A (v1): RA-1.1 (vi) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002368 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-01 |
| **Definition:** | The organization defines the personnel or roles to whom the risk assessment policy is disseminated. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): RA-1 a 1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002369 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-01 |
| **Definition:** | The organization defines the personnel or roles to whom the risk assessment procedures are disseminated. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): RA-1 a 2 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001039 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization reviews and updates the current risk assessment policy in accordance with organization-defined frequency. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): RA-1 a<br>NIST: NIST SP 800-53 Revision 4 (v4): RA-1 b 1<br>NIST: NIST SP 800-53A (v1): RA-1.2 (ii) | | |

**CCI:** CCI-001040 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization defines the frequency with which to review and update the current risk assessment policy.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): RA-1 a
NIST: NIST SP 800-53 Revision 4 (v4): RA-1 b 1
NIST: NIST SP 800-53A (v1): RA-1.2 (i)

---

**CCI:** CCI-001043 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization reviews and updates the current risk assessment procedures in accordance with organization-defined frequency.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): RA-1 b
NIST: NIST SP 800-53 Revision 4 (v4): RA-1 b 2
NIST: NIST SP 800-53A (v1): RA-1.2 (iv)

---

**CCI:** CCI-001044 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization defines the frequency with which to review and update the current risk assessment procedures.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): RA-1 b
NIST: NIST SP 800-53 Revision 4 (v4): RA-1 b 2
NIST: NIST SP 800-53A (v1): RA-1.2 (iii)

---

**CCI:** CCI-001045 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): RA-2 a
NIST: NIST SP 800-53 Revision 4 (v4): RA-2 a
NIST: NIST SP 800-53A (v1): RA-2.1 (i)

---

**CCI:** CCI-001046 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization documents the security categorization results (including supporting rationale) in the security plan for the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): RA-2 b
NIST: NIST SP 800-53 Revision 4 (v4): RA-2 b
NIST: NIST SP 800-53A (v1): RA-2.1 (ii)

---

**CCI:** CCI-001047 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization ensures the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): RA-2 c
NIST: NIST SP 800-53 Revision 4 (v4): RA-2 c
NIST: NIST SP 800-53A (v1): RA-2.1 (iii)

---

**CCI:** CCI-001048 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization conducts an assessment of risk of the information system and the information it processes, stores, or transmits that includes the likelihood and magnitude of harm from the unauthorized access, use, disclosure, disruption, modification, or destruction.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): RA-3 a
NIST: NIST SP 800-53 Revision 4 (v4): RA-3 a
NIST: NIST SP 800-53A (v1): RA-3.1 (i)

---

**CCI:** CCI-001642 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2010-05-12

**Definition:** The organization defines the organizational document in which risk assessment results are documented (e.g., security plan, risk assessment report).

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): RA-3 b
NIST: NIST SP 800-53 Revision 4 (v4): RA-3 b
NIST: NIST SP 800-53A (v1): RA-3.1 (ii)

---

**CCI:** CCI-001049 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization documents risk assessment results in the organization-defined document.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): RA-3 b

NIST: NIST SP 800-53 Revision 4 (v4): RA-3 b
NIST: NIST SP 800-53A (v1): RA-3.1 (iii)

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-001050 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |

**Definition:** The organization reviews risk assessment results on an organization-defined frequency.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): RA-3 c
NIST: NIST SP 800-53 Revision 4 (v4): RA-3 c
NIST: NIST SP 800-53A (v1): RA-3.1 (v)

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-001051 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |

**Definition:** The organization defines a frequency for reviewing risk assessment results.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): RA-3 c
NIST: NIST SP 800-53 Revision 4 (v4): RA-3 c
NIST: NIST SP 800-53A (v1): RA-3.1 (iv)

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-002370 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-01 |

**Definition:** The organization disseminates risk assessment results to organization-defined personnel or roles.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): RA-3 d

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-002371 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-01 |

**Definition:** The organization defines the personnel or roles to whom the risk assessment results will be disseminated.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): RA-3 d

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-001052 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |

**Definition:** The organization updates the risk assessment on an organization-defined frequency or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

| | |
|---|---|
| **Type:** | policy |
| **References:** | NIST: NIST SP 800-53 (v3): RA-3 d<br>NIST: NIST SP 800-53 Revision 4 (v4): RA-3 e<br>NIST: NIST SP 800-53A (v1): RA-3 |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001053 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization defines a frequency for updating the risk assessment. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): RA-3 d<br>NIST: NIST SP 800-53 Revision 4 (v4): RA-3 e<br>NIST: NIST SP 800-53A (v1): RA-3 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001641 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-12 |
| **Definition:** | The organization defines the process for conducting random vulnerability scans on the information system and hosted applications. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): RA-5 a<br>NIST: NIST SP 800-53 Revision 4 (v4): RA-5 a<br>NIST: NIST SP 800-53A (v1): RA-5.1 (i) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001643 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-12 |
| **Definition:** | The organization scans for vulnerabilities in the information system and hosted applications in accordance with the organization-defined process for random scans. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): RA-5 b<br>NIST: NIST SP 800-53 Revision 4 (v4): RA-5 a<br>NIST: NIST SP 800-53A (v1): RA-5.1 (ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001054 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization scans for vulnerabilities in the information system and hosted applications on an organization-defined frequency. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): RA-5 a<br>NIST: NIST SP 800-53 Revision 4 (v4): RA-5 a<br>NIST: NIST SP 800-53A (v1): RA-5.1 (ii) | | |

---

**CCI:** CCI-001055 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization defines a frequency for scanning for vulnerabilities in the information system and hosted applications.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): RA-5 a
NIST: NIST SP 800-53 Revision 4 (v4): RA-5 a
NIST: NIST SP 800-53A (v1): RA-5.1 (i)

---

**CCI:** CCI-001056 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization scans for vulnerabilities in the information system and hosted applications when new vulnerabilities potentially affecting the system/applications are identified and reported.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): RA-5 a
NIST: NIST SP 800-53 Revision 4 (v4): RA-5 a
NIST: NIST SP 800-53A (v1): RA-5.1 (iii)

---

**CCI:** CCI-001057 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: enumerating platforms, software flaws, and improper configurations; formatting checklists and test procedures; and measuring vulnerability impact.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): RA-5 b
NIST: NIST SP 800-53 Revision 4 (v4): RA-5 b
NIST: NIST SP 800-53A (v1): RA-5.1 (iv)

---

**CCI:** CCI-001058 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization analyzes vulnerability scan reports and results from security control assessments.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): RA-5 c
NIST: NIST SP 800-53 Revision 4 (v4): RA-5 c
NIST: NIST SP 800-53A (v1): RA-5.1 (v)

---

**CCI:** CCI-001059 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization remediates legitimate vulnerabilities in organization-defined response times in accordance with an organizational assessment risk.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): RA-5 d
NIST: NIST SP 800-53 Revision 4 (v4): RA-5 d
NIST: NIST SP 800-53A (v1): RA-5.2 (ii)

---

**CCI:** CCI-001060 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization defines response times for remediating legitimate vulnerabilities in accordance with an organization assessment of risk.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): RA-5 d
NIST: NIST SP 800-53 Revision 4 (v4): RA-5 d
NIST: NIST SP 800-53A (v1): RA-5.2 (i)

---

**CCI:** CCI-001061 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization shares information obtained from the vulnerability scanning process and security control assessments with organization-defined personnel or roles to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): RA-5 e
NIST: NIST SP 800-53 Revision 4 (v4): RA-5 e
NIST: NIST SP 800-53A (v1): RA-5.2 (iii)

---

**CCI:** CCI-002376 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization defines the personnel or roles with whom the information obtained from the vulnerability scanning process and security control assessments will be shared.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): RA-5 e

---

**CCI:** CCI-001062 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization employs vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): RA-5 (1)
NIST: NIST SP 800-53 Revision 4 (v4): RA-5 (1)
NIST: NIST SP 800-53A (v1): RA-5 (1).1

---

**CCI:** CCI-001063 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization updates the information system vulnerabilities scanned on an organization-defined frequency, prior to a new scan, and/or when new vulnerabilities are identified and reported.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): RA-5 (2)
NIST: NIST SP 800-53 Revision 4 (v4): RA-5 (2)
NIST: NIST SP 800-53A (v1): RA-5 (2).1 (ii)

---

**CCI:** CCI-001064 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization defines a frequency for updating the information system vulnerabilities scanned.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): RA-5 (2)
NIST: NIST SP 800-53 Revision 4 (v4): RA-5 (2)
NIST: NIST SP 800-53A (v1): RA-5 (2).1 (i)

---

**CCI:** CCI-002373 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-07-01
**Definition:** The organization employs vulnerability scanning procedures that can identify the breadth and depth of coverage (i.e., information system components scanned and vulnerabilities checked).
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): RA-5 (3)

---

**CCI:** CCI-001066 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization determines what information about the information system is discoverable by adversaries.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): RA-5 (4)
NIST: NIST SP 800-53 Revision 4 (v4): RA-5 (4)
NIST: NIST SP 800-53A (v1): RA-5 (4).1

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002374 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-01 |
| **Definition:** | The organization defines the corrective actions when information about the information system is discoverable by adversaries. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): RA-5 (4) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002375 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |
| **Definition:** | The organization takes organization-defined corrective actions when information about the information system is discoverable by adversaries. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): RA-5 (4) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001645 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-12 |
| **Definition:** | The organization identifies the information system components to which privileged access is authorized for selected organization-defined vulnerability scanning activities. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): RA-5 (5)<br>NIST: NIST SP 800-53 Revision 4 (v4): RA-5 (5)<br>NIST: NIST SP 800-53A (v1): RA-5 (5).1 (i) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001067 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The information system implements privileged access authorization to organization-identified information system components for selected organization-defined vulnerability scanning activities. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): RA-5 (5)<br>NIST: NIST SP 800-53 Revision 4 (v4): RA-5 (5)<br>NIST: NIST SP 800-53A (v1): RA-5 (5).1 (ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002906 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-08-13 |
| **Definition:** | The organization defines the vulnerability scanning activities in which the information system implements privileged access authorization to organization-identified information system components. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): RA-5 (5) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001068 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization employs automated mechanisms to compare the results of vulnerability scans over time to determine trends in information system vulnerabilities. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): RA-5 (6)<br>NIST: NIST SP 800-53 Revision 4 (v4): RA-5 (6)<br>NIST: NIST SP 800-53A (v1): RA-5 (6).1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001071 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization reviews historic audit logs to determine if a vulnerability identified in the information system has been previously exploited. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): RA-5 (8)<br>NIST: NIST SP 800-53 Revision 4 (v4): RA-5 (8)<br>NIST: NIST SP 800-53A (v1): RA-5 (8).1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002372 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-01 |
| **Definition:** | The organization correlates the output from vulnerability scanning tools to determine the presence of multi-vulnerability/multi-hop attack vectors. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): RA-5 (10) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003119 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-23 |
| **Definition:** | The organization employs a technical surveillance countermeasures survey at organization-defined locations on an organization-defined frequency or when organization-defined events or indicators occur. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): RA-6 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003120 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-23 |
| **Definition:** | The organization defines the locations where technical surveillance countermeasures surveys are to be employed. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): RA-6 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003121 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-23 |
| **Definition:** | The organization defines the frequency on which to employ technical surveillance countermeasures surveys. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): RA-6 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003122 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-23 |
| **Definition:** | The organization defines the events or indicators upon which technical surveillance countermeasures surveys are to be employed. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): RA-6 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000602 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization develops and documents a system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SA-1 a<br>NIST: NIST SP 800-53 Revision 4 (v4): SA-1 a 1<br>NIST: NIST SP 800-53A (v1): SA-1.1 (i) (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000603 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization disseminates to organization-defined personnel or roles a system and services acquisition policy. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SA-1 a<br>NIST: NIST SP 800-53 Revision 4 (v4): SA-1 a 1<br>NIST: NIST SP 800-53A (v1): SA-1.1 (iii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000605 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization develops and documents procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls. | | |
| **Type:** | policy | | |

**References:** NIST: NIST SP 800-53 (v3): SA-1 b
NIST: NIST SP 800-53 Revision 4 (v4): SA-1 a 2
NIST: NIST SP 800-53A (v1): SA-1.1 (iv) (v)

---

**CCI:** CCI-000606 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization disseminates to organization-defined personnel or roles procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): SA-1 b
NIST: NIST SP 800-53 Revision 4 (v4): SA-1 a 2
NIST: NIST SP 800-53A (v1): SA-1.1 (vi)

---

**CCI:** CCI-003089 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-09-23
**Definition:** The organization defines the personnel or roles to whom the system and services acquisition policy is disseminated.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-1 a 1

---

**CCI:** CCI-003090 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-09-23
**Definition:** The organization defines the personnel or roles to whom procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls are disseminated.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-1 a 2

---

**CCI:** CCI-000601 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization defines the frequency with which to review and update the current system and services acquisition policy.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): SA-1
NIST: NIST SP 800-53 Revision 4 (v4): SA-1 b 1
NIST: NIST SP 800-53A (v1): SA-1.2 (i)

---

**CCI:** CCI-000604 **Status:** draft
**Contributor:** DISA FSO **Published** 2009-09-21

**Date:**

**Definition:** The organization reviews and updates the current system and services acquisition policy in accordance with organization-defined frequency.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-1 a
NIST: NIST SP 800-53 Revision 4 (v4): SA-1 b 1
NIST: NIST SP 800-53A (v1): SA-1.2 (ii)

---

**CCI:** CCI-000607 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization reviews and updates the current system and services acquisition procedures in accordance with organization-defined frequency.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-1 b
NIST: NIST SP 800-53 Revision 4 (v4): SA-1 b 2
NIST: NIST SP 800-53A (v1): SA-1.2 (iv)

---

**CCI:** CCI-001646 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2010-05-12

**Definition:** The organization defines the frequency with which to review and update the current system and services acquisition procedures.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-1
NIST: NIST SP 800-53 Revision 4 (v4): SA-1 b 2
NIST: NIST SP 800-53A (v1): SA-1.2 (iii)

---

**CCI:** CCI-003091 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-23

**Definition:** The organization determines information security requirements for the information system or information system service in mission/business process planning.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-2 a

---

**CCI:** CCI-000610 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization determines the resources required to protect the information system or information system service as part of its capital planning and investment control process.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-2 b
NIST: NIST SP 800-53 Revision 4 (v4): SA-2 b

NIST: NIST SP 800-53A (v1): SA-2.1 (ii)

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000611 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization documents the resources required to protect the information system or information system service as part of its capital planning and investment control process. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SA-2 b<br>NIST: NIST SP 800-53 Revision 4 (v4): SA-2 b<br>NIST: NIST SP 800-53A (v1): SA-2.1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000612 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SA-2 b<br>NIST: NIST SP 800-53 Revision 4 (v4): SA-2 b<br>NIST: NIST SP 800-53A (v1): SA-2.1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000613 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization establishes a discrete line item for information security in organizational programming documentation. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SA-2 c<br>NIST: NIST SP 800-53 Revision 4 (v4): SA-2 c<br>NIST: NIST SP 800-53A (v1): SA-2.1 (iii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000614 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization establishes a discrete line item for information security in organizational budgeting documentation. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SA-2 c<br>NIST: NIST SP 800-53 Revision 4 (v4): SA-2 c<br>NIST: NIST SP 800-53A (v1): SA-2.1 (iii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000615 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published** | 2009-09-21 |

| | | | |
|---|---|---|---|
| | | **Date:** | |
| **Definition:** | The organization manages the information system using an organization-defined system development life cycle that incorporates information security considerations. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SA-3 a<br>NIST: NIST SP 800-53 Revision 4 (v4): SA-3 a<br>NIST: NIST SP 800-53A (v1): SA-3.1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003092 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-23 |
| **Definition:** | The organization defines a system development life cycle that is used to manage the information system. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SA-3 a | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000616 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization defines and documents information system security roles and responsibilities throughout the system development life cycle. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SA-3 b<br>NIST: NIST SP 800-53 Revision 4 (v4): SA-3 b<br>NIST: NIST SP 800-53A (v1): SA-3.1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000618 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization identifies individuals having information system security roles and responsibilities. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SA-3 c<br>NIST: NIST SP 800-53 Revision 4 (v4): SA-3 c<br>NIST: NIST SP 800-53A (v1): SA-3.1 (iii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003093 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-23 |
| **Definition:** | The organization integrates the organizational information security risk management process into system development life cycle activities. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SA-3 d | | |

**CCI:** CCI-003094 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-23

**Definition:** The organization includes the security functional requirements, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-4 a

---

**CCI:** CCI-003095 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-23

**Definition:** The organization includes the security strength requirements, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-4 b

---

**CCI:** CCI-003096 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-23

**Definition:** The organization includes the security assurance requirements, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-4 c

---

**CCI:** CCI-003097 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-23

**Definition:** The organization includes the security-related documentation requirements, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-4 d

---

**CCI:** CCI-003098 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-23

**Definition:** The organization includes requirements for protecting security-related documentation, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-4 e

---

**CCI:** CCI-003099 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-23

**Definition:** The organization includes description of the information system development environment and environment in which the system is intended to operate, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-4 f

---

**CCI:** CCI-003100 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-23

**Definition:** The organization includes acceptance criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-4 g

---

**CCI:** CCI-000623 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-4 (1)
NIST: NIST SP 800-53 Revision 4 (v4): SA-4 (1)
NIST: NIST SP 800-53A (v1): SA-4 (1).1

---

**CCI:** CCI-003101 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-23

**Definition:** The organization requires the developer of the information system, system component, or information system service to provide design information for the security controls to be employed that includes security-relevant external system interfaces, high-level design, low-level design, source code, hardware schematics, and/or organization-defined design information at an organization-defined level of detail.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-4 (2)

---

**CCI:** CCI-003102 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-23

**Definition:** The organization requires the developer of the information system, system component, or information system service to provide implementation information for the security controls to be employed that includes security-relevant external system interfaces, high-level design, low-level design, source code, hardware schematics, and/or organization-defined implementation information at an organization-defined level of detail.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-4 (2)

---

**CCI:** CCI-003103 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-23

**Definition:** The organization defines the design information that the developer of the information system, system component, or information system service is required to provide for the security controls to be employed.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-4 (2)

---

**CCI:** CCI-003104 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-23

**Definition:** The organization defines the implementation information that the developer of the information system, system component, or information system service is required to provide for the security controls to be employed.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-4 (2)

---

**CCI:** CCI-003105 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-23

**Definition:** The organization defines the level of detail for the design information of the security controls that is required to be provided by the developer of the information system, system component, or information system services.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-4 (2)

---

**CCI:** CCI-003106 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-23

**Definition:** The organization defines the level of detail for the implementation information of the security controls that is required to be provided by the developer of the information system, system component, or information system services.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-4 (2)

---

**CCI:** CCI-003107 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-23

**Definition:** The organization requires the developer of the information system, system component, or information system service to demonstrate the use of a system development life cycle that includes organization-defined state-of-the-practice system/security engineering methods, software development methods, testing/evaluation/validation techniques, and quality control processes.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-4 (3)

---

**CCI:** CCI-003108 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-23

**Definition:** The organization defines the state-of-the-practice system/security engineering methods, software development methods, testing/evaluation/validation techniques, and quality control processes that the developer of the information system, system component, or information system service is required to include when demonstrating the use of a system development life cycle.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-4 (3)

---

**CCI:** CCI-003109 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-23

**Definition:** The organization requires the developer of the information system, system component, or information system service to deliver the system, component, or service with organization-defined security configurations implemented.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-4 (5) (a)

---

**CCI:** CCI-003110 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-23

**Definition:** The organization defines the security configurations required to be implemented when the developer delivers the information system, system component, or information system service.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-4 (5) (a)

---

**CCI:** CCI-003111 **Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2013-09-23

**Definition:** The organization requires the developer of the information system, system component, or information system service to use the organization-defined security configurations as the default for any subsequent system, component, or service reinstallation or upgrade.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-4 (5) (b)

---

**CCI:** CCI-000631

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2009-09-21

**Definition:** The organization employs only government off-the-shelf (GOTS) or commercial off-the-shelf (COTS) information assurance (IA) and IA-enabled information technology products that compose an NSA-approved solution to protect classified information when the networks used to transmit the information are at a lower classification level than the information being transmitted.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-4 (6) (a)

NIST: NIST SP 800-53 Revision 4 (v4): SA-4 (6) (a)

NIST: NIST SP 800-53A (v1): SA-4 (6).1 (i)

---

**CCI:** CCI-000633

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2009-09-21

**Definition:** The organization ensures that government off-the-shelf (GOTS) or commercial-off-the-shelf(COTS) information assurance (IA) and IA-enabled information technology products have been evaluated and/or validated by the NSA or in accordance with NSA-approved procedures.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-4 (6) (b)

NIST: NIST SP 800-53 Revision 4 (v4): SA-4 (6) (b)

NIST: NIST SP 800-53A (v1): SA-4 (6).1 (ii)

---

**CCI:** CCI-000634

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2009-09-21

**Definition:** The organization limits the use of commercially provided information assurance (IA) and IA-enabled information technology products to those products that have been successfully evaluated against a National Information Assurance Partnership (NIAP)-approved Protection Profile for a specific technology type, if such a profile exists.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-4 (7) (a)

NIST: NIST SP 800-53 Revision 4 (v4): SA-4 (7) (a)

NIST: NIST SP 800-53A (v1): SA-4 (7).1 (i)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000635 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization requires, if no NIAP-approved Protection Profile exists for a specific technology type but a commercially provided information technology product relies on cryptographic functionality to enforce its security policy, that the cryptographic module is FIPS-validated. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SA-4 (7) (b)<br>NIST: NIST SP 800-53 Revision 4 (v4): SA-4 (7) (b)<br>NIST: NIST SP 800-53A (v1): SA-4 (7).1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003112 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-23 |
| **Definition:** | The organization requires the developer of the information system, system component, or information system service to produce a plan for the continuous monitoring of security control effectiveness that contains an organization-defined level of detail. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SA-4 (8) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003113 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-23 |
| **Definition:** | The organization defines the level of detail to be contained in the plan for the continuous monitoring of security control effectiveness that the developer of the information system, system component, or information system services is required to produce. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SA-4 (8) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003114 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-23 |
| **Definition:** | The organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SA-4 (9) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003115 | **Status:** | deprecated |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-23 |
| **Definition:** | The organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use. | | |

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-4 (9)

---

**CCI:** CCI-003116 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-23

**Definition:** The organization employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-4 (10)

---

**CCI:** CCI-003124 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization obtains administrator documentation for the information system, system component, or information system service that describes secure configuration of the system, component, or service.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-5 a 1

---

**CCI:** CCI-003125 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization obtains administrator documentation for the information system, system component, or information system service that describes secure installation of the system, component, or service.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-5 a 1

---

**CCI:** CCI-003126 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization obtains administrator documentation for the information system, system component, or information system service that describes secure operation of the system, component, or service.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-5 a 1

---

**CCI:** CCI-003127 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization obtains administrator documentation for the information system, system component, or information system services that describes effective use and maintenance of security functions/mechanisms.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-5 a 2

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003128 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-30 |

**Definition:** The organization obtains administrator documentation for the information system, system component, or information system service that describes known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-5 a 3

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003129 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-30 |

**Definition:** The organization obtains user documentation for the information system, system component, or information system service that describes user-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-5 b 1

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003130 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-30 |

**Definition:** The organization obtains user documentation for the information system, system component, or information system service that describes methods for user interaction which enables individuals to use the system, component, or service in a more secure manner.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-5 b 2

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003131 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-30 |

**Definition:** The organization obtains user documentation for the information system, system component, or information system service that describes user responsibilities in maintaining the security of the system, component, or service.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-5 b 3

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000642 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |

**Definition:** The organization documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-5 b
NIST: NIST SP 800-53 Revision 4 (v4): SA-5 c
NIST: NIST SP 800-53A (v1): SA-5.1 (iii)

---

**CCI:** CCI-003132 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization takes organization-defined actions in response to attempts to obtain either unavailable or nonexistent documentation for the information system, system component, or information system service.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-5 c

---

**CCI:** CCI-003133 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization defines actions to be taken in response to attempts to obtain either unavailable or nonexistent documentation for the information system, system component, or information system service.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-5 c

---

**CCI:** CCI-003134 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization protects information system, system component, or information system service documentation as required, in accordance with the risk management strategy.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-5 d

---

**CCI:** CCI-003135 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization distributes information system, system component, or information system service documentation to organization-defined personnel or roles.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-5 e

---

**CCI:** CCI-003136 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization defines the personnel or roles to whom information system, system component, or information system service documentation is to be distributed.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-5 e

---

**CCI:** CCI-000664 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization applies information system security engineering principles in the specification of the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-8

NIST: NIST SP 800-53 Revision 4 (v4): SA-8

NIST: NIST SP 800-53A (v1): SA-8.1 (i)

---

**CCI:** CCI-000665 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization applies information system security engineering principles in the design of the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-8

NIST: NIST SP 800-53 Revision 4 (v4): SA-8

NIST: NIST SP 800-53A (v1): SA-8.1 (ii)

---

**CCI:** CCI-000666 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization applies information system security engineering principles in the development of the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-8

NIST: NIST SP 800-53 Revision 4 (v4): SA-8

NIST: NIST SP 800-53A (v1): SA-8.1 (iii)

---

**CCI:** CCI-000667 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization applies information system security engineering principles in the implementation of the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-8

NIST: NIST SP 800-53 Revision 4 (v4): SA-8

NIST: NIST SP 800-53A (v1): SA-8.1 (iv)

---

**CCI:** CCI-000668 **Status:** draft

**Contributor:** DISA FSO **Published** 2009-09-21

**Date:**

**Definition:** The organization applies information system security engineering principles in the modification of the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-8
NIST: NIST SP 800-53 Revision 4 (v4): SA-8
NIST: NIST SP 800-53A (v1): SA-8.1 (v)

---

**CCI:** CCI-003140 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-9 (1) (a)

---

**CCI:** CCI-000669 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization requires that providers of external information system services comply with organizational information security requirements.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-9 a
NIST: NIST SP 800-53 Revision 4 (v4): SA-9 a
NIST: NIST SP 800-53A (v1): SA-9.1 (i)

---

**CCI:** CCI-000670 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization requires that providers of external information system services employ organization-defined security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-9 a
NIST: NIST SP 800-53 Revision 4 (v4): SA-9 a
NIST: NIST SP 800-53A (v1): SA-9.1 (i)

---

**CCI:** CCI-003137 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization defines security controls that providers of external information system services employ in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-9 a

---

**CCI:** CCI-000671 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization defines government oversight with regard to external information system services.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): SA-9 b
NIST: NIST SP 800-53 Revision 4 (v4): SA-9 b
NIST: NIST SP 800-53A (v1): SA-9.1 (ii)

---

**CCI:** CCI-000672 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization documents government oversight with regard to external information system services.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): SA-9 b
NIST: NIST SP 800-53 Revision 4 (v4): SA-9 b
NIST: NIST SP 800-53A (v1): SA-9.1 (ii)

---

**CCI:** CCI-000673 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization defines user roles and responsibilities with regard to external information system services.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): SA-9 b
NIST: NIST SP 800-53 Revision 4 (v4): SA-9 b
NIST: NIST SP 800-53A (v1): SA-9.1 (ii)

---

**CCI:** CCI-000674 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization documents user roles and responsibilities with regard to external information system services.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): SA-9 b
NIST: NIST SP 800-53 Revision 4 (v4): SA-9 b
NIST: NIST SP 800-53A (v1): SA-9.1 (ii)

---

**CCI:** CCI-003138 **Status:** draft
**Contributor:** DISA FSO **Published** 2013-09-30

**Date:**

**Definition:** The organization employs organization-defined processes, methods, and techniques to monitor security control compliance by external service providers on an ongoing basis.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-9 c

---

**CCI:** CCI-003139 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization defines processes, methods, and techniques to employ to monitor security control compliance by external service providers on an ongoing basis.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-9 c

---

**CCI:** CCI-003141 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization ensures that the acquisition or outsourcing of dedicated information security services is approved by organization-defined personnel or roles.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-9 (1) (b)

---

**CCI:** CCI-003142 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization defines the personnel or roles authorized to approve the acquisition or outsourcing of dedicated information security services.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-9 (1) (b)

---

**CCI:** CCI-003143 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization requires providers of organization-defined external information system services to identify the functions, ports, protocols, and other services required for the use of such services.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-9 (2)

---

**CCI:** CCI-003144 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization defines the external information system services for which the providers are required to identify the functions, ports, protocols, and other services required for the use of such services.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-9 (2)

---

**CCI:** CCI-003145 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization establishes trust relationships with external service providers based on organization-defined security requirements, properties, factors, or conditions defining acceptable trust relationships.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-9 (3)

---

**CCI:** CCI-003146 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization documents trust relationships with external service providers based on organization-defined security requirements, properties, factors, or conditions defining acceptable trust relationships.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-9 (3)

---

**CCI:** CCI-003147 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization maintains trust relationships with external service providers based on organization-defined security requirements, properties, factors, or conditions defining acceptable trust relationships.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-9 (3)

---

**CCI:** CCI-003148 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization defines security requirements, properties, factors, or conditions defining acceptable trust relationships with external service providers.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-9 (3)

---

**CCI:** CCI-003149 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization employs organization-defined security safeguards to ensure that the interests of organization-defined external service providers are consistent with and reflect organizational interests.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-9 (4)

---

**CCI:** CCI-003150 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization defines security safeguards to employ to ensure that the interests of organization-defined external service providers are consistent with and reflect organizational interests.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-9 (4)

---

**CCI:** CCI-003151 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization defines external service providers whose interests are consistent with and reflect organizational interests.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-9 (4)

---

**CCI:** CCI-003152 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization restricts the location of information processing, information/data, and/or information system services to organization-defined locations based on organization-defined requirements or conditions.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-9 (5)

---

**CCI:** CCI-003153 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization defines the locations for which to restrict information processing, information/data, and/or information system services based on organization-defined requirements or conditions.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-9 (5)

---

**CCI:** CCI-003154 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization defines the requirements or conditions on which to base restricting the location of information processing, information/data, and/or information system services to organization-defined locations.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-9 (5)

---

**CCI:** CCI-003155 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization requires the developer of the information system, system component, or information system service to perform configuration management during system, component, or service design, development, implementation and/or operation.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-10 a

---

**CCI:** CCI-003156 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization requires the developer of the information system, system component, or information system service to document the integrity of changes to organization-defined configuration items under configuration management.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-10 b

---

**CCI:** CCI-003157 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization requires the developer of the information system, system component, or information system service to manage the integrity of changes to organization-defined configuration items under configuration management.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-10 b

---

**CCI:** CCI-003158 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization requires the developer of the information system, system component, or information system service to control the integrity of changes to organization-defined configuration items under configuration management.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-10 b

---

**CCI:** CCI-003159 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization defines the configuration items under configuration management that require the integrity of changes to be documented, managed and controlled.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-10 b

---

**CCI:** CCI-000692 **Status:** draft

**Contributor:** DISA FSO
**Published Date:** 2009-09-22

**Definition:** The organization requires the developer of the information system, system component, or information system service to implement only organization-approved changes to the system, component, or service.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-10 (c)
NIST: NIST SP 800-53 Revision 4 (v4): SA-10 c
NIST: NIST SP 800-53A (v1): SA-10.1 (iii)

---

**CCI:** CCI-000694
**Status:** draft

**Contributor:** DISA FSO
**Published Date:** 2009-09-22

**Definition:** The organization requires the developer of the information system, system component, or information system service to document approved changes to the system, component, or service.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-10 (d)
NIST: NIST SP 800-53 Revision 4 (v4): SA-10 d
NIST: NIST SP 800-53A (v1): SA-10.1 (iv)

---

**CCI:** CCI-003160
**Status:** draft

**Contributor:** DISA FSO
**Published Date:** 2013-09-30

**Definition:** The organization requires the developer of the information system, system component, or information system service to document the potential security impacts of approved changes to the system, component, or service.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-10 d

---

**CCI:** CCI-003161
**Status:** draft

**Contributor:** DISA FSO
**Published Date:** 2013-09-30

**Definition:** The organization requires the developer of the information system, system component, or information system service to track security flaws within the system, component, or service.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-10 e

---

**CCI:** CCI-003162
**Status:** draft

**Contributor:** DISA FSO
**Published Date:** 2013-09-30

**Definition:** The organization requires the developer of the information system, system component, or information system service to track flaw resolution within the system, component, or service.

**Type:** policy

| | | | |
|---|---|---|---|
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SA-10 e | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003163 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-30 |
| **Definition:** | The organization requires the developer of the information system, system component, or information system service to report findings of security flaws and flaw resolution within the system, component, or service to organization-defined personnel. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SA-10 e | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003164 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-30 |
| **Definition:** | The organization defines the personnel to whom security flaw findings and flaw resolution within the system, component, or service are reported. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SA-10 e | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000698 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization requires the developer of the information system, system component, or information system service to enable integrity verification of software and firmware components. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SA-10 (1)<br>NIST: NIST SP 800-53 Revision 4 (v4): SA-10 (1)<br>NIST: NIST SP 800-53A (v1): SA-10 (1).1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000700 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization provides an alternate configuration management process using organizational personnel in the absence of a dedicated developer configuration management team. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SA-10 (2)<br>NIST: NIST SP 800-53 Revision 4 (v4): SA-10 (2)<br>NIST: NIST SP 800-53A (v1): SA-10 (2).1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003165 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-30 |
| **Definition:** | The organization requires the developer of the information system, system component, or | | |

information system service to enable integrity verification of hardware components.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-10 (3)

---

**CCI:** CCI-003166 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization requires the developer of the information system, system component, or information system service to employ tools for comparing newly generated versions of security-relevant hardware descriptions with previous versions.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-10 (4)

---

**CCI:** CCI-003167 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization requires the developer of the information system, system component, or information system service to employ tools for comparing newly generated versions of software/firmware source code with previous versions.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-10 (4)

---

**CCI:** CCI-003168 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization requires the developer of the information system, system component, or information system service to employ tools for comparing newly generated versions of object code with previous versions.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-10 (4)

---

**CCI:** CCI-003169 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization requires the developer of the information system, system component, or information system service to maintain the integrity of the mapping between the master build data (hardware drawings and software/firmware code) describing the current version of security-relevant hardware, software, and firmware and the on-site master copy of the data for the current version.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-10 (5)

---

**CCI:** CCI-003170 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization requires the developer of the information system, system component, or information system service to execute procedures for ensuring that security-relevant hardware, software, and firmware updates distributed to the organization are exactly as specified by the master copies.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-10 (6)

---

**CCI:** CCI-003171 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization requires the developer of the information system, system component, or information system service to create a security assessment plan.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-11 a

---

**CCI:** CCI-003172 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization requires the developer of the information system, system component, or information system service to implement a security assessment plan.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-11 a

---

**CCI:** CCI-003173 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization requires the developer of the information system, system component, or information system service to perform unit, integration, system, and/or regression testing/evaluation at an organization-defined depth and coverage.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-11 b

---

**CCI:** CCI-003174 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization defines the depth and coverage at which to perform unit, integration, system, and/or regression testing/evaluation.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-11 b

---

**CCI:** CCI-003175 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization requires the developer of the information system, system component, or information system service to produce evidence of the execution of the security assessment plan.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-11 c

---

**CCI:** CCI-003176 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization requires the developer of the information system, system component, or information system service to produce the results of the security testing/evaluation.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-11 c

---

**CCI:** CCI-003177 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization requires the developer of the information system, system component, or information system service to implement a verifiable flaw remediation process.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-11 d

---

**CCI:** CCI-003178 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization requires the developer of the information system, system component, or information system service to correct flaws identified during security testing/evaluation.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-11 e

---

**CCI:** CCI-003179 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization requires the developer of the information system, system component, or information system service to employ static code analysis tools to identify common flaws.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-11 (1)

---

**CCI:** CCI-003180 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization requires the developer of the information system, system component, or information system service to document the results of static code analysis.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-11 (1)

---

**CCI:** CCI-003181 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization requires the developer of the information system, system component, or information system service to perform threat and vulnerability analysis.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-11 (2)

---

**CCI:** CCI-003182 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization requires the developer of the information system, system component, or information system service to perform testing/evaluation of the as-built system, component, or service subsequent to threat and vulnerability analysis.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-11 (2)

---

**CCI:** CCI-003183 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization requires an independent agent satisfying organization-defined independence criteria to verify the correct implementation of the developer security assessment plan.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-11 (3) (a)

---

**CCI:** CCI-003184 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization requires an independent agent satisfying organization-defined independence criteria to verify the evidence produced during security testing/evaluation.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-11 (3) (a)

---

**CCI:** CCI-003185 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization defines the independence criteria the independent agent must satisfy prior to verifying the correct implementation of the developer security assessment plan and the evidence produced during security testing/evaluation.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-11 (3) (a)

---

**CCI:** CCI-003186 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization ensures that the independent agent either is provided with sufficient information to complete the verification process or has been granted the authority to obtain such information.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-11 (3) (b)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003187 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-30 |

**Definition:** The organization requires the developer of the information system, system component, or information system service to perform a manual code review of organization-defined specific code using organization-defined processes, procedures, and/or techniques.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-11 (4)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003188 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-30 |

**Definition:** The organization defines the specific code for which the developer of the information system, system component, or information system service is required to perform a manual code review using organization-defined process, procedures, and/or techniques.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-11 (4)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003189 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-30 |

**Definition:** The organization defines the processes, procedures, and/or techniques to be used by the developer of the information system, system component, or information system service to perform a manual code review of organization-defined specific code.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-11 (4)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003190 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-30 |

**Definition:** The organization requires the developer of the information system, system component, or information system service to perform penetration testing at an organization-defined breadth/depth and with organization-defined constraints.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-11 (5)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003191 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-30 |

**Definition:** The organization defines the breadth/depth at which the developer of the information system, system component, or information system service is required to perform penetration testing.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-11 (5)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003192 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-30 |

**Definition:** The organization defines the constraints on penetration testing performed by the developer of the information system, system component, or information system service.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-11 (5)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003193 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-30 |

**Definition:** The organization requires the developer of the information system, system component, or information system service to perform attack surface reviews.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-11 (6)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003194 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-30 |

**Definition:** The organization requires the developer of the information system, system component, or information system service to verify that the scope of security testing/evaluation provides complete coverage of required security controls at an organization-defined depth of testing/evaluation.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-11 (7)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003195 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-30 |

**Definition:** The organization defines the depth of testing/evaluation to which the developer of the information system, system component, or information system service is required to verify that the scope of security testing/evaluation provides complete coverage of the required security controls.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-11 (7)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003196 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-30 |

**Definition:** The organization requires the developer of the information system, system component, or information system service to employ dynamic code analysis tools to identify common flaws.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-11 (8)

---

**CCI:** CCI-003197 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization requires the developer of the information system, system component, or information system service to document the results of the dynamic code analysis.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-11 (8)

---

**CCI:** CCI-000722 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization defines the security safeguards to employ to protect against supply chain threats to the information system, system component, or information system service.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-12
NIST: NIST SP 800-53 Revision 4 (v4): SA-12
NIST: NIST SP 800-53A (v1): SA-12.1 (i)

---

**CCI:** CCI-000723 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization protects against supply chain threats to the information system, system component, or information system service by employing organization-defined security safeguards as part of a comprehensive, defense-in-breadth information security strategy.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-12
NIST: NIST SP 800-53 Revision 4 (v4): SA-12
NIST: NIST SP 800-53A (v1): SA-12.1 (ii)

---

**CCI:** CCI-003198 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization employs organization-defined tailored acquisition strategies, contract tools, and procurement methods for the purchase of the information system, system component, or information system service from suppliers.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-12 (1)

---

**CCI:** CCI-003199 **Status:** draft

| | | | |
|---|---|---|---|
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-30 |
| **Definition:** | The organization defines tailored acquisition strategies, contract tools, and procurement methods to employ for the purchase of the information system, system component, or information system service from suppliers. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SA-12 (1) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003207 | **Status:** | deprecated |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-30 |
| **Definition:** | The organization employs organization-defined tailored acquisition strategies, contract tools, and procurement methods for the purchase of the information system, system component, or information system service from suppliers. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SA-12 (1) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003208 | **Status:** | deprecated |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-30 |
| **Definition:** | The organization employs organization-defined tailored acquisition strategies, contract tools, and procurement methods for the purchase of the information system, system component, or information system service from suppliers. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SA-12 (1) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003209 | **Status:** | deprecated |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-30 |
| **Definition:** | The organization employs organization-defined tailored acquisition strategies, contract tools, and procurement methods for the purchase of the information system, system component, or information system service from suppliers. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SA-12 (1) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003200 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-30 |
| **Definition:** | The organization conducts a supplier review prior to entering into a contractual agreement to acquire the information system, system component, or information system service. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SA-12 (2) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003201 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published** | 2013-09-30 |

| | | | |
|---|---|---|---|
| | | **Date:** | |
| **Definition:** | The organization employs organization-defined security safeguards to limit harm from potential adversaries identifying and targeting the organizational supply chain. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SA-12 (5) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003202 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-30 |
| **Definition:** | The organization defines security safeguards to employ to limit harm from potential adversaries identifying and targeting the organizational supply chain. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SA-12 (5) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003203 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-30 |
| **Definition:** | The organization conducts an assessment of the information system, system component, or information system service prior to selection, acceptance, or update. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SA-12 (7) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003204 | **Status:** | deprecated |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-30 |
| **Definition:** | The organization conducts an assessment of the information system, system component, or information system service prior to selection, acceptance, or update. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SA-12 (7) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003205 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-30 |
| **Definition:** | The organization uses all-source intelligence analysis of suppliers and potential suppliers of the information system, system component, or information system service. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SA-12 (8) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003206 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-30 |
| **Definition:** | The organization employs organization-defined Operations Security (OPSEC) safeguards in accordance with classification guides to protect supply chain-related information for the information system, system component, or information system service. | | |
| **Type:** | policy | | |

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-12 (9)

---

**CCI:** CCI-003210 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization defines the Operations Security (OPSEC) safeguards to be employed in accordance with classification guides to protect supply chain-related information for the information system, system component, or information system service.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-12 (9)

---

**CCI:** CCI-003211 **Status:** deprecated

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization defines the Operations Security (OPSEC) safeguards to be employed in accordance with classification guides to protect supply chain-related information for the information system, system component, or information system service.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-12 (9)

---

**CCI:** CCI-003212 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization employs organization-defined security safeguards to validate that the information system or system component received is genuine and has not been altered.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-12 (10)

---

**CCI:** CCI-003213 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization defines the security safeguards to be employed to validate that the information system or system component received is genuine and has not been altered.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-12 (10)

---

**CCI:** CCI-003214 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization employs organizational analysis, independent third-party analysis, organizational penetration testing and/or independent third-party penetration testing of organization-defined supply chain elements, processes, and actors associated with the information system, system component, or information system service.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-12 (11)

---

**CCI:** CCI-003215 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-09-30
**Definition:** The organization defines the supply chain elements, processes, and actors associated with the information system, system component, or information system service for organizational analysis, independent third-party analysis, organizational penetration testing and/or independent third-party penetration testing.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-12 (11)

---

**CCI:** CCI-003216 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-09-30
**Definition:** The organization establishes inter-organizational agreements with entities involved in the supply chain for the information system, system component, or information system service.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-12 (12)

---

**CCI:** CCI-003217 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-09-30
**Definition:** The organization establishes inter-organizational procedures with entities involved in the supply chain for the information system, system component, or information system service.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-12 (12)

---

**CCI:** CCI-003218 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-09-30
**Definition:** The organization employs organization-defined security safeguards to ensure an adequate supply of organization-defined critical information system components.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-12 (13)

---

**CCI:** CCI-003219 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-09-30
**Definition:** The organization defines the security safeguards to be employed to ensure an adequate supply of organization-defined critical information system components.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-12 (13)

---

**CCI:** CCI-003220 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization defines the critical information system components for which organization-defined security safeguards are employed to ensure adequate supply.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-12 (13)

---

**CCI:** CCI-003221 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization establishes unique identification of organization-defined supply chain elements, processes, and actors for the information system, system component, or information system service.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-12 (14)

---

**CCI:** CCI-003222 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization retains unique identification of organization-defined supply chain elements, processes, and actors for the information system, system component, or information system service.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-12 (14)

---

**CCI:** CCI-003223 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization defines the supply chain elements, processes, and actors for the information system, system component, or information system service to establish and retain unique identification.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-12 (14)

---

**CCI:** CCI-003224 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization establishes a process to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-12 (15)

---

**CCI:** CCI-003225 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization describes the trustworthiness required in the organization-defined information system, information system component, or information system service supporting its critical missions/business functions.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-13 a

---

**CCI:** CCI-003226 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization defines the information system, information system component, or information system service supporting its critical missions/business functions in which the trustworthiness must be described.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-13 a

---

**CCI:** CCI-003227 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization implements an organization-defined assurance overlay to achieve trustworthiness required to support its critical missions/business functions.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-13 b

---

**CCI:** CCI-003228 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization defines an assurance overlay to be implemented to achieve trustworthiness required to support its critical missions/business functions.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-13 b

---

**CCI:** CCI-003229 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization identifies critical information system components by performing a criticality analysis for organization-defined information systems, information system components, or information system services at organization-defined decision points in the system development life cycle.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-14

---

**CCI:** CCI-003230 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization identifies critical information system functions by performing a criticality analysis for organization-defined information systems, information system components, or information system services at organization-defined decision points in the system development life cycle.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-14

---

**CCI:** CCI-003231 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization defines the information systems, information system components, or information system services for which the organization identifies critical information system components and functions for criticality analysis.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-14

---

**CCI:** CCI-003232 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization defines the decision points in the system development life cycle at which to perform a criticality analysis to identify critical information system components and functions for organization-defined information systems, information system components, or information system services.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-14

---

**CCI:** CCI-003233 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization requires the developer of the information system, system component, or information system service to follow a documented development process.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-15

---

**CCI:** CCI-003234 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The documented information system, system component, or information system service development process explicitly addresses security requirements.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-15 a 1

---

**CCI:** CCI-003235 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The documented information system, system component, or information system service development process identifies the standards used in the development process.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-15 a 2

---

**CCI:** CCI-003236 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The documented information system, system component, or information system service development process identifies the tools used in the development process.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-15 a 2

---

**CCI:** CCI-003237 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The documented information system, system component, or information system service development process documents the specific tool options and tool configurations used in the development process.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-15 a 3

---

**CCI:** CCI-003238 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The documented information system, system component, or information system service development process documents changes to the process and/or tools used in development.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-15 a 4

---

**CCI:** CCI-003239 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The documented information system, system component, or information system service development process manages changes to the process and/or tools used in development.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-15 a 4

---

**CCI:** CCI-003240 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The documented information system, system component, or information system service development process ensures the integrity of changes to the process and/or tools used in development.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-15 a 4

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-003241 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-30 |
| **Definition:** | The organization reviews the development process in accordance with organization-defined frequency to determine if the development process selected and employed can satisfy organization-defined security requirements. |  |  |
| **Type:** | policy |  |  |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SA-15 b |  |  |

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-003242 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-30 |
| **Definition:** | The organization reviews the development standards in accordance with organization-defined frequency to determine if the development standards selected and employed can satisfy organization-defined security requirements. |  |  |
| **Type:** | policy |  |  |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SA-15 b |  |  |

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-003243 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-30 |
| **Definition:** | The organization reviews the development tools in accordance with organization-defined frequency to determine if the development tools selected and employed can satisfy organization-defined security requirements. |  |  |
| **Type:** | policy |  |  |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SA-15 b |  |  |

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-003244 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-30 |
| **Definition:** | The organization reviews the development tool options/configurations in accordance with organization-defined frequency to determine if the development tool options/configurations selected and employed can satisfy organization-defined security requirements. |  |  |
| **Type:** | policy |  |  |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SA-15 b |  |  |

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-003245 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-30 |
| **Definition:** | The organization defines the frequency on which to review the development process, standards, tools, and tool options/configurations to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy organization-defined security requirements. |  |  |
| **Type:** | policy |  |  |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SA-15 b |  |  |

**CCI:** CCI-003246 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization defines the security requirements that must be satisfied by conducting a review of the development process, standards, tools, and tool options/configurations.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-15 b

---

**CCI:** CCI-003247 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization requires the developer of the information system, system component, or information system service to define quality metrics at the beginning of the development process.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-15 (1) (a)

---

**CCI:** CCI-003248 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization requires the developer of the information system, system component, or information system service to provide evidence of meeting the quality metrics in accordance with organization-defined frequency, organization-defined program review milestones and/or upon delivery.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-15 (1) (b)

---

**CCI:** CCI-003249 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization defines the frequency on which the developer of the information system, system component, or information system service is required to provide evidence of meeting the quality metrics.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-15 (1) (b)

---

**CCI:** CCI-003250 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization defines the program review milestones at which the developer of the information system, system component, or information system service is required to provide evidence of meeting the quality metrics.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-15 (1) (b)

---

**CCI:** CCI-003251

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2013-09-30

**Definition:** The organization requires the developer of the information system, system component, or information system service to select a security tracking tool for use during the development process.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-15 (2)

---

**CCI:** CCI-003252

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2013-09-30

**Definition:** The organization requires the developer of the information system, system component, or information system service to employ a security tracking tool for use during the development process.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-15 (2)

---

**CCI:** CCI-003253

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2013-09-30

**Definition:** The organization requires the developer of the information system, system component, or information system service to perform a criticality analysis at an organization-defined breadth/depth and at organization-defined decision points in the system development life cycle.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-15 (3)

---

**CCI:** CCI-003254

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2013-09-30

**Definition:** The organization defines the breadth/depth at which the developer of the information system, system component, or information system service is required to perform a criticality analysis.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-15 (3)

---

**CCI:** CCI-003255

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2013-09-30

**Definition:** The organization defines decision points in the system development life cycle at which the developer of the information system, system component, or information system service is required to perform a criticality analysis.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-15 (3)

---

**CCI:** CCI-003256

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2013-09-30

**Definition:** The organization requires that developers perform threat modeling for the information system at an organization-defined breadth/depth.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-15 (4)

---

**CCI:** CCI-003257

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2013-09-30

**Definition:** The organization requires that developers perform a vulnerability analysis for the information system at an organization-defined breadth/depth.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-15 (4)

---

**CCI:** CCI-003258

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2013-09-30

**Definition:** The organization defines the breadth/depth at which threat modeling for the information system must be performed by developers.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-15 (4)

---

**CCI:** CCI-003259

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2013-09-30

**Definition:** The organization defines the breadth/depth at which vulnerability analysis for the information system must be performed by developers.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-15 (4)

---

**CCI:** CCI-003260

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2013-09-30

**Definition:** Threat modeling performed by the developer for the information system uses organization-defined information concerning impact, environment of operations, known or assumed threats, and acceptable risk levels.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-15 (4) (a)

---

**CCI:** CCI-003261

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2013-09-30

**Definition:** Vulnerability analysis performed by the developer for the information system uses

| | |
|---|---|
| | organization-defined information concerning impact, environment of operations, known or assumed threats, and acceptable risk levels. |
| **Type:** | policy |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SA-15 (4) (a) |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003262 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-30 |
| **Definition:** | The organization defines information concerning impact, environment of operations, known or assumed threats, and acceptable risk levels to be used to perform threat modeling for the information system by the developer. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SA-15 (4) (a) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003263 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-30 |
| **Definition:** | The organization defines information concerning impact, environment of operations, known or assumed threats, and acceptable risk levels to be used to perform a vulnerability analysis for the information system by the developer. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SA-15 (4) (a) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003264 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-30 |
| **Definition:** | The organization requires the threat modeling performed by the developers employ organization-defined tools and methods. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SA-15 (4) (b) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003265 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-30 |
| **Definition:** | The organization requires the vulnerability analysis performed by the developers employ organization-defined tools and methods. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SA-15 (4) (b) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003266 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-09-30 |
| **Definition:** | The organization defines tools and methods to be employed to perform threat modeling for the information system by the developer. | | |
| **Type:** | policy | | |

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-15 (4) (b)

---

**CCI:** CCI-003267 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization defines tools and methods to be employed to perform a vulnerability analysis for the information system by the developer.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-15 (4) (b)

---

**CCI:** CCI-003268 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization requires that developers performing threat modeling for the information system produce evidence that meets organization-defined acceptance criteria.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-15 (4) (c)

---

**CCI:** CCI-003269 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization requires that developers performing vulnerability analysis for the information system produce evidence that meets organization-defined acceptance criteria.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-15 (4) (c)

---

**CCI:** CCI-003270 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-09-30

**Definition:** The organization defines the acceptance criteria that must be met when threat modeling of the information system is performed by the developer.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-15 (4) (c)

---

**CCI:** CCI-003271 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization defines the acceptance criteria that must be met when vulnerability analysis of the information system is performed by the developer.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-15 (4) (c)

---

**CCI:** CCI-003272 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization requires the developer of the information system, system component, or information system service to reduce attack surfaces to organization-defined thresholds.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-15 (5)

---

**CCI:** CCI-003273 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization defines the thresholds to which the developer of the information system, system component, or information system service is required to reduce attack surfaces.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-15 (5)

---

**CCI:** CCI-003274 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization requires the developer of the information system, system component, or information system service to implement an explicit process to continuously improve the development process.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-15 (6)

---

**CCI:** CCI-003275 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization requires the developer of the information system, system component, or information system services to perform an automated vulnerability analysis using organization-defined tools.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-15 (7) (a)

---

**CCI:** CCI-003276 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization defines the tools the developer of the information system, system component, or information system services uses to perform an automated vulnerability analysis.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-15 (7) (a)

---

**CCI:** CCI-003277 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization requires the developer of the information system, system component, or information system services to determine the exploitation potential for discovered vulnerabilities.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-15 (7) (b)

---

**CCI:** CCI-003278 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization requires the developer of the information system, system component, or information system services to determine potential risk mitigations for delivered vulnerabilities.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-15 (7) (c)

---

**CCI:** CCI-003279 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization requires the developer of the information system, system component, or information system services to deliver the outputs of the tools and results of the vulnerability analysis to organization-defined personnel or roles.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-15 (7) (d)

---

**CCI:** CCI-003280 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization defines the personnel or roles to whom the outputs of the tools and results of the vulnerability analysis are delivered.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-15 (7) (d)

---

**CCI:** CCI-003281 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization requires the developer of the information system, system component, or information system service to use threat modeling from similar systems, components, or services to inform the current development process.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-15 (8)

---

**CCI:** CCI-003282 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization requires the developer of the information system, system component, or information system service to use vulnerability analysis from similar systems, components, or services to inform the current development process.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-15 (8)

---

**CCI:** CCI-003283 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization approves the use of live data in development environments for the information system, system component, or information system service.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-15 (9)

---

**CCI:** CCI-003284 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization approves the use of live data in test environments for the information system, system component, or information system service.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-15 (9)

---

**CCI:** CCI-003285 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization documents the use of live data in development environments for the information system, system component, or information system service.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-15 (9)

---

**CCI:** CCI-003286 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization documents the use of live data in test environments for the information system, system component, or information system service.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-15 (9)

---

**CCI:** CCI-003287 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization controls the use of live data in development environments for the information system, system component, or information system service.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-15 (9)

---

**CCI:** CCI-003288 **Status:** draft

**Contributor:** DISA FSO **Published** 2013-10-03

**Date:**

**Definition:** The organization controls the use of live data in test environments for the information system, system component, or information system service.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-15 (9)

---

**CCI:** CCI-003289 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization requires the developer of the information system, system component, or information system service to provide an incident response plan.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-15 (10)

---

**CCI:** CCI-003290 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization requires the developer of the information system or system component to archive the system or component to be released or delivered together with the corresponding evidence supporting the final security review.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-15 (11)

---

**CCI:** CCI-003291 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization requires the developer of the information system, system component, or information system service to provide organization-defined training on the correct use and operation of the implemented security functions, controls, and/or mechanisms.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-16

---

**CCI:** CCI-003292 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization defines the training the developer of the information system, system component, or information system service is required to provide on the correct use and operation of the implemented security functions, controls, and/or mechanisms.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-16

---

**CCI:** CCI-003293 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization requires the developer of the information system, system component, or information system service to produce a design specification and security architecture.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17

---

**CCI:** CCI-003294 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The design specification and security architecture is consistent with and supportive of the organization's security architecture which is established within and is an integrated part of the organization's enterprise architecture.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17 a

---

**CCI:** CCI-003295 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The design specification and security architecture accurately and completely describes the required security functionality.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17 b

---

**CCI:** CCI-003296 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The design specification and security architecture accurately and completely describes the allocation of security controls among physical and logical components.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17 b

---

**CCI:** CCI-003297 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The design specification and security architecture expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17 c

---

**CCI:** CCI-003298 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization requires the developer of the information system, system component, or information system to produce, as an integral part of the development process, a formal policy model describing the organization-defined elements of organizational security policy to be enforced.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17 (1) (a)

---

**CCI:** CCI-003299 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization defines the elements of organization security policy to be described in the formal policy model for enforcement on the information system, system component, or information system service.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17 (1) (a)

---

**CCI:** CCI-003300 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization requires the developer of the information system, system component, or information system service to prove that the formal policy model is internally consistent and sufficient to enforce the defined elements of the organizational security policy when implemented.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17 (1) (b)

---

**CCI:** CCI-003301 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization requires the developer of the information system, system component, or information system service to define security-relevant hardware.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17 (2) (a)

---

**CCI:** CCI-003302 **Status:** deprecated

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization requires the developer of the information system, system component, or information system service to define security-relevant hardware.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17 (2) (a)

---

**CCI:** CCI-003303 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization requires the developer of the information system, system component, or information system service to define security-relevant software.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17 (2) (a)

**CCI:** CCI-003304 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization requires the developer of the information system, system component, or information system service to define security-relevant firmware.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17 (2) (a)

---

**CCI:** CCI-003305 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization requires the developer of the information system, system component, or information system service to provide a rationale that the definition for security-relevant hardware is complete.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17 (2) (a)

---

**CCI:** CCI-003306 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization requires the developer of the information system, system component, or information system service to provide a rationale that the definition for security-relevant software is complete.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17 (2) (b)

---

**CCI:** CCI-003307 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization requires the developer of the information system, system component, or information system service to provide a rationale that the definition for security-relevant firmware is complete.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17 (2) (b)

---

**CCI:** CCI-003308 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization requires the developer of the information system, system component, or information system service to produce, as an integral part of the development process, a formal top-level specification that specifies the interfaces to security-relevant hardware in terms of exceptions, error messages, and effects.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17 (3) (a)

---

**CCI:** CCI-003309
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2013-10-03
**Definition:** The organization requires the developer of the information system, system component, or information system service to produce, as an integral part of the development process, a formal top-level specification that specifies the interfaces to security-relevant software in terms of exceptions, error messages, and effects.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17 (3) (a)

---

**CCI:** CCI-003310
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2013-10-03
**Definition:** The organization requires the developer of the information system, system component, or information system service to produce, as an integral part of the development process, a formal top-level specification that specifies the interfaces to security-relevant firmware in terms of exceptions, error messages, and effects.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17 (3) (a)

---

**CCI:** CCI-003311
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2013-10-03
**Definition:** The organization requires the developer of the information system, system component, or information system service to show via proof to the extent feasible with additional informal demonstration as necessary, that the formal top-level specification is consistent with the formal policy model.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17 (3) (b)

---

**CCI:** CCI-003312
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2013-10-03
**Definition:** The organization requires the developer of the information system, system component, or information system service to show via informal demonstration, that the formal top-level specification completely covers the interfaces to security-relevant hardware.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17 (3) (c)

---

**CCI:** CCI-003313
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2013-10-03
**Definition:** The organization requires the developer of the information system, system component, or information system service to show via informal demonstration, that the formal top-level specification completely covers the interfaces to security-relevant software.
**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17 (3) (c)

---

**CCI:** CCI-003314 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization requires the developer of the information system, system component, or information system service to show via informal demonstration, that the formal top-level specification completely covers the interfaces to security-relevant firmware.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17 (3) (c)

---

**CCI:** CCI-003315 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization requires the developer of the information system, system component, or information system service to show that the formal top-level specification is an accurate description of the implemented security-relevant hardware.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17 (3) (d)

---

**CCI:** CCI-003316 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization requires the developer of the information system, system component, or information system service to show that the formal top-level specification is an accurate description of the implemented security-relevant software.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17 (3) (d)

---

**CCI:** CCI-003317 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization requires the developer of the information system, system component, or information system service to show that the formal top-level specification is an accurate description of the implemented security-relevant firmware.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17 (3) (d)

---

**CCI:** CCI-003318 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization requires the developer of the information system, system component, or information system service to describe the security-relevant hardware mechanisms not addressed in the formal top-level specification but strictly internal to the security-relevant hardware.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17 (3) (e)

---

**CCI:** CCI-003319

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2013-10-03

**Definition:** The organization requires the developer of the information system, system component, or information system service to describe the security-relevant software mechanisms not addressed in the formal top-level specification but strictly internal to the security-relevant software.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17 (3) (e)

---

**CCI:** CCI-003320

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2013-10-03

**Definition:** The organization requires the developer of the information system, system component, or information system service to describe the security-relevant firmware mechanisms not addressed in the formal top-level specification but strictly internal to the security-relevant firmware.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17 (3) (e)

---

**CCI:** CCI-003321

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2013-10-03

**Definition:** The organization requires the developer of the information system, system component, or information system service to produce, as an integral part of the development process, an informal descriptive top-level specification that specifies the interfaces to security-relevant hardware in terms of exceptions, error messages, and effects.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17 (4) (a)

---

**CCI:** CCI-003322

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2013-10-03

**Definition:** The organization requires the developer of the information system, system component, or information system service to produce, as an integral part of the development process, an informal descriptive top-level specification that specifies the interfaces to security-relevant software in terms of exceptions, error messages, and effects.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17 (4) (a)

---

**CCI:** CCI-003323

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2013-10-03

**Definition:** The organization requires the developer of the information system, system component, or information system service to produce, as an integral part of the development process, an informal descriptive top-level specification that specifies the interfaces to security-relevant firmware in terms of exceptions, error messages, and effects.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17 (4) (a)

---

**CCI:** CCI-003324 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization requires the developer of the information system, system component, or information system service to show via informal demonstration or convincing argument with formal methods as feasible that the descriptive top-level specification is consistent with the formal policy model.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17 (4) (b)

---

**CCI:** CCI-003325 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization requires the developer of the information system, system component, or information system service to show via informal demonstration, that the descriptive top-level specification completely covers the interfaces to security-relevant hardware.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17 (4) (c)

---

**CCI:** CCI-003326 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization requires the developer of the information system, system component, or information system service to show via informal demonstration, that the descriptive top-level specification completely covers the interfaces to security-relevant software.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17 (4) (c)

---

**CCI:** CCI-003327 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization requires the developer of the information system, system component, or information system service to show via informal demonstration, that the descriptive top-level specification completely covers the interfaces to security-relevant firmware.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17 (4) (c)

---

**CCI:** CCI-003328 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization requires the developer of the information system, system component, or information system service to show that the descriptive top-level specification is an accurate description of the interfaces to security-relevant hardware.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17 (4) (d)

---

**CCI:** CCI-003329 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization requires the developer of the information system, system component, or information system service to show that the descriptive top-level specification is an accurate description of the interfaces to security-relevant software.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17 (4) (d)

---

**CCI:** CCI-003330 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization requires the developer of the information system, system component, or information system service to show that the descriptive top-level specification is an accurate description of the interfaces to security-relevant firmware.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17 (4) (d)

---

**CCI:** CCI-003331 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization requires the developer of the information system, system component, or information system service to describe the security-relevant hardware mechanisms not addressed in the descriptive top-level specification but strictly internal to the security-relevant hardware.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17 (4) (e)

---

**CCI:** CCI-003332 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization requires the developer of the information system, system component, or information system service to describe the security-relevant software mechanisms not addressed in the descriptive top-level specification but strictly internal to the security-relevant software.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17 (4) (e)

---

**CCI:** CCI-003333 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization requires the developer of the information system, system component, or information system service to describe the security-relevant firmware mechanisms not addressed in the descriptive top-level specification but strictly internal to the security-relevant firmware.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17 (4) (e)

---

**CCI:** CCI-003334 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization requires the developer of the information system, system component, or information system service to design and structure the security-relevant hardware to use a complete, conceptually simple protection mechanism with precisely defined semantics.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17 (5) (a)

---

**CCI:** CCI-003335 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization requires the developer of the information system, system component, or information system service to design and structure the security-relevant software to use a complete, conceptually simple protection mechanism with precisely defined semantics.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17 (5) (a)

---

**CCI:** CCI-003336 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization requires the developer of the information system, system component, or information system service to design and structure the security-relevant firmware to use a complete, conceptually simple protection mechanism with precisely defined semantics.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17 (5) (a)

---

**CCI:** CCI-003337 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization requires the developer of the information system, system component, or information system service to internally structure the security-relevant hardware with specific regard for the complete, conceptually simple protection mechanism with precisely defined semantics.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17 (5) (b)

---

**CCI:** CCI-003338 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-10-03
**Definition:** The organization requires the developer of the information system, system component, or information system service to internally structure the security-relevant software with specific regard for the complete, conceptually simple protection mechanism with precisely defined semantics.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17 (5) (b)

---

**CCI:** CCI-003339 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-10-03
**Definition:** The organization requires the developer of the information system, system component, or information system service to internally structure the security-relevant firmware with specific regard for the complete, conceptually simple protection mechanism with precisely defined semantics.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17 (5) (b)

---

**CCI:** CCI-003340 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-10-03
**Definition:** The organization requires the developer of the information system, component, or information system service to structure security-relevant hardware to facilitate testing.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17 (6)

---

**CCI:** CCI-003341 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-10-03
**Definition:** The organization requires the developer of the information system, component, or information system service to structure security-relevant software to facilitate testing.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17 (6)

---

**CCI:** CCI-003342 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-10-03
**Definition:** The organization requires the developer of the information system, component, or information system service to structure security-relevant firmware to facilitate testing.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17 (6)

---

**CCI:** CCI-003343 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-10-03
**Definition:** The organization requires the developer of the information system, component, or information system service to structure security-relevant hardware to facilitate controlling access with least privilege.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17 (7)

---

**CCI:** CCI-003344 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-10-03
**Definition:** The organization requires the developer of the information system, component, or information system service to structure security-relevant software to facilitate controlling access with least privilege.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17 (7)

---

**CCI:** CCI-003345 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-10-03
**Definition:** The organization requires the developer of the information system, component, or information system service to structure security-relevant firmware to facilitate controlling access with least privilege.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-17 (7)

---

**CCI:** CCI-003346 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-10-03
**Definition:** The organization implements a tamper protection program for the information system, system component, or information system service.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-18

---

**CCI:** CCI-003347 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-10-03
**Definition:** The organization employs anti-tamper technologies and techniques during multiple phases in the system development life cycle including design.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-18 (1)

---

**CCI:** CCI-003348 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization employs anti-tamper technologies and techniques during multiple phases in the system development life cycle including development.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-18 (1)

---

**CCI:** CCI-003349 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization employs anti-tamper technologies and techniques during multiple phases in the system development life cycle including integration.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-18 (1)

---

**CCI:** CCI-003350 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization employs anti-tamper technologies and techniques during multiple phases in the system development life cycle including operations.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-18 (1)

---

**CCI:** CCI-003351 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization employs anti-tamper technologies and techniques during multiple phases in the system development life cycle including maintenance.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-18 (1)

---

**CCI:** CCI-003352 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization inspects organization-defined information systems, system components, or devices at random, at an organization-defined frequency, and/or upon organization-defined indications of need for inspection to detect tampering.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-18 (2)

---

**CCI:** CCI-003353 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization defines the information systems, system components, or devices to inspect at random, at an organization-defined frequency, and/or upon organization-defined indications of need for inspection to detect tampering.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-18 (2)

---

**CCI:** CCI-003354 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization defines the frequency on which to inspect organization-defined information systems, system components, or devices to detect tampering.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-18 (2)

---

**CCI:** CCI-003355 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization defines indications of need for inspection to detect tampering during inspections of organization-defined information systems, system components, or devices.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-18 (2)

---

**CCI:** CCI-003356 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization develops an anti-counterfeit policy that includes the means to detect counterfeit components from entering the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-19 a

---

**CCI:** CCI-003357 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization develops an anti-counterfeit policy that includes the means to prevent counterfeit components from entering the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-19 a

---

**CCI:** CCI-003358 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization develops anti-counterfeit procedures that include the means to detect counterfeit components from entering the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-19 a

---

**CCI:** CCI-003359 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization develops anti-counterfeit procedures that include the means to prevent counterfeit components from entering the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-19 a

---

**CCI:** CCI-003360 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization implements an anti-counterfeit policy that includes the means to detect counterfeit components from entering the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-19 a

---

**CCI:** CCI-003361 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization implements an anti-counterfeit policy that includes the means to prevent counterfeit components from entering the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-19 a

---

**CCI:** CCI-003362 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization implements anti-counterfeit procedures that include the means to detect counterfeit components from entering the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-19 a

---

**CCI:** CCI-003363 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization implements anti-counterfeit procedures that include the means to prevent counterfeit components from entering the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-19 a

---

**CCI:** CCI-003364 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization reports counterfeit information system components to the source of the counterfeit component, organization-defined external reporting organizations, and/or organization-defined personnel or roles.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-19 b

---

**CCI:** CCI-003365 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization defines the external reporting organizations to which counterfeit information system components are to be reported.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-19 b

---

**CCI:** CCI-003366 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization defines the personnel or roles to whom counterfeit information system components are to be reported.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-19 b

---

**CCI:** CCI-003367 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization trains organization-defined personnel or roles to detect counterfeit information system components (including hardware, software, and firmware).

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-19 (1)

---

**CCI:** CCI-003368 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization defines the personnel or roles to be trained to detect counterfeit information system components (including hardware, software, and firmware).

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-19 (1)

---

**CCI:** CCI-003369 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization maintains configuration control over organization-defined information system components awaiting service/repair.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-19 (2)

---

**CCI:** CCI-003370 **Status:** draft

**Contributor:** DISA FSO **Published** 2013-10-03

**Date:**

**Definition:** The organization defines the information system components awaiting service/repair over which configuration control must be maintained.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-19 (2)

---

**CCI:** CCI-003371 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization maintains configuration control over serviced/repaired components awaiting return to service.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-19 (2)

---

**CCI:** CCI-003390 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization defines the techniques and methods used to dispose of information system components.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-19 (3)

---

**CCI:** CCI-003391 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization disposes of information system components using organization-defined techniques and methods.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-19 (3)

---

**CCI:** CCI-003388 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization defines the frequency on which to scan for counterfeit information system components.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-19 (4)

---

**CCI:** CCI-003389 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization scans for counterfeit information system components in accordance with organization-defined frequency.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-19 (4)

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003386 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-10-03 |
| **Definition:** | The organization defines the critical information system components to re-implement or custom develop. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SA-20 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003387 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-10-03 |
| **Definition:** | The organization re-implements or custom develops organization-defined critical information system components. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SA-20 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003383 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-10-03 |
| **Definition:** | The organization defines the official government duties to be assigned to the developer of an organization-defined information system, system component, or information system service. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SA-21 a | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003385 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-10-03 |
| **Definition:** | The organization requires that the developer of an organization-defined information system, system component, or information system service have appropriate access authorizations as determined by assigned organization-defined official government duties. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SA-21 a | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003381 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-10-03 |
| **Definition:** | The organization defines additional personnel screening criteria that must be satisfied by the developer of an organization-defined information system, system component, or information system service. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SA-21 b | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003382 | **Status:** | draft |

| | | | |
|---|---|---|---|
| **Contributor:** | DISA FSO | **Published Date:** | 2013-10-03 |
| **Definition:** | The organization requires that the developer of an organization-defined information system, system component, or information system service satisfy organization-defined additional personnel screening criteria. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SA-21 b | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003377 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-10-03 |
| **Definition:** | The organization defines the actions the developer of the information system, system component, or information system service must take to ensure the required screening criteria are satisfied. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SA-21 (1) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003378 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-10-03 |
| **Definition:** | The organization defines the actions the developer of the information system, system component, or information system service must take to ensure the required access authorizations are satisfied. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SA-21 (1) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003379 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-10-03 |
| **Definition:** | The organization requires the developer of the information system, system component, or information system service take organization-defined actions to ensure the required screening criteria are satisfied. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SA-21 (1) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003380 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-10-03 |
| **Definition:** | The organization requires the developer of the information system, system component, or information system service take organization-defined actions to ensure the required access authorizations are satisfied. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SA-21 (1) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003384 | **Status:** | draft |

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization defines the information system, system component, or information system service which requires the information system developer to have appropriate access authorizations and satisfy additional personnel screening criteria.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-21

---

**CCI:** CCI-003376 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization replaces information system components when support for the components is no longer available from the developer, vendor, or manufacturer.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-22 a

---

**CCI:** CCI-003374 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization documents approval for the continued use of unsupported system components required to satisfy mission/business needs.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-22 b

---

**CCI:** CCI-003375 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization provides justification for the continued use of unsupported system components required to satisfy mission/business needs.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-22 b

---

**CCI:** CCI-003372 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization defines the support from external providers to be provided for unsupported information system components.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-22 (1)

---

**CCI:** CCI-003373 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-10-03

**Definition:** The organization provides in-house support and/or organization-defined support from external providers for unsupported information system components.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SA-22 (1)

---

**CCI:** CCI-001074 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization develops a system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-1 a
NIST: NIST SP 800-53 Revision 4 (v4): SC-1 a 1
NIST: NIST SP 800-53A (v1): SC-1.1 (i) (ii)

---

**CCI:** CCI-001075 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization disseminates to organization-defined personnel or roles the system and communications protection policy.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-1 a
NIST: NIST SP 800-53 Revision 4 (v4): SC-1 a 1
NIST: NIST SP 800-53A (v1): SC-1.1 (iii)

---

**CCI:** CCI-001078 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization develops system and communications protection procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-1 b
NIST: NIST SP 800-53 Revision 4 (v4): SC-1 a 2
NIST: NIST SP 800-53A (v1): SC-1.1 (iv) (v)

---

**CCI:** CCI-001079 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization disseminates to organization-defined personnel or roles the procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-1 b
NIST: NIST SP 800-53 Revision 4 (v4): SC-1 a 2

NIST: NIST SP 800-53A (v1): SC-1.1 (vi)

---

**CCI:** CCI-002377 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization documents the system and communications protection policy.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-1 a 1

---

**CCI:** CCI-002378 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization defines the personnel or roles to be recipients of the system and communications protection policy.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-1 a 1

---

**CCI:** CCI-002379 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization documents procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-1 a 2

---

**CCI:** CCI-002380 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization defines the personnel or roles to be recipients of the procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-1 a 2

---

**CCI:** CCI-001076 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization reviews and updates the system and communications protection policy in accordance with organization-defined frequency.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-1 a
NIST: NIST SP 800-53 Revision 4 (v4): SC-1 b 1
NIST: NIST SP 800-53A (v1): SC-1.2 (ii)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001077 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |

**Definition:** The organization defines the frequency for reviewing and updating the system and communications protection policy.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-1 a
NIST: NIST SP 800-53 Revision 4 (v4): SC-1 b 1
NIST: NIST SP 800-53A (v1): SC-1.2 (i)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001080 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |

**Definition:** The organization reviews and updates the system and communications protection procedures in accordance with organization-defined frequency.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-1 b
NIST: NIST SP 800-53 Revision 4 (v4): SC-1 b 2
NIST: NIST SP 800-53A (v1): SC-1.2 (iv)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001081 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |

**Definition:** The organization defines the frequency of system and communications protection procedure reviews and updates.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-1 b
NIST: NIST SP 800-53 Revision 4 (v4): SC-1 b 2
NIST: NIST SP 800-53A (v1): SC-1.2 (iii)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001082 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |

**Definition:** The information system separates user functionality (including user interface services) from information system management functionality.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SC-2
NIST: NIST SP 800-53 Revision 4 (v4): SC-2
NIST: NIST SP 800-53A (v1): SC-2.1

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001083 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |

**Definition:** The information system prevents the presentation of information system management-related functionality at an interface for non-privileged users.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SC-2 (1)
NIST: NIST SP 800-53 Revision 4 (v4): SC-2 (1)
NIST: NIST SP 800-53A (v1): SC-2 (1).1

---

**CCI:** CCI-001084 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The information system isolates security functions from nonsecurity functions.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SC-3
NIST: NIST SP 800-53 Revision 4 (v4): SC-3
NIST: NIST SP 800-53A (v1): SC-3.1 (ii)

---

**CCI:** CCI-001085 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The information system utilizes underlying hardware separation mechanisms to implement security function isolation.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SC-3 (1)
NIST: NIST SP 800-53 Revision 4 (v4): SC-3 (1)
NIST: NIST SP 800-53A (v1): SC-3 (1).1

---

**CCI:** CCI-001086 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The information system isolates security functions enforcing access and information flow control from both nonsecurity functions and from other security functions.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SC-3 (2)
NIST: NIST SP 800-53 Revision 4 (v4): SC-3 (2)
NIST: NIST SP 800-53A (v1): SC-3 (2).1

---

**CCI:** CCI-002381 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization minimizes the number of nonsecurity functions included within the isolation boundary containing security functions.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-3 (3)

---

**CCI:** CCI-002382 **Status:** draft

|  |  |  |  |
|---|---|---|---|
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |
| **Definition:** | The organization implements security functions as largely independent modules that maximize internal cohesiveness within modules and minimize coupling between modules. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SC-3 (4) | | |

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-001089 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization implements security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): SC-3 (5)<br>NIST: NIST SP 800-53 Revision 4 (v4): SC-3 (5)<br>NIST: NIST SP 800-53A (v1): SC-3 (5).1 | | |

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-001090 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The information system prevents unauthorized and unintended information transfer via shared system resources. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): SC-4<br>NIST: NIST SP 800-53 Revision 4 (v4): SC-4<br>NIST: NIST SP 800-53A (v1): SC-4.1 | | |

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-002383 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |
| **Definition:** | The organization defines the procedures to be employed to prevent unauthorized information transfer via shared resources when system processing explicitly switches between different information classification levels or security categories. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SC-4 (2) | | |

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-002384 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |
| **Definition:** | The information system prevents unauthorized information transfer via shared resources in accordance with organization-defined procedures when system processing explicitly switches between different information classification levels or security categories. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SC-4 (2) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001093 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization defines the types of denial of service attacks (or provides references to sources of current denial of service attacks) that can be addressed by the information system. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SC-5<br>NIST: NIST SP 800-53 Revision 4 (v4): SC-5<br>NIST: NIST SP 800-53A (v1): SC-5.1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002385 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |
| **Definition:** | The information system protects against or limits the effects of organization-defined types of denial of service attacks by employing organization-defined security safeguards. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SC-5 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002386 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |
| **Definition:** | The organization defines the security safeguards to be employed to protect the information system against, or limit the effects of, denial of service attacks. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SC-5 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001094 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The information system restricts the ability of individuals to launch organization-defined denial of service attacks against other information systems. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): SC-5 (1)<br>NIST: NIST SP 800-53 Revision 4 (v4): SC-5 (1)<br>NIST: NIST SP 800-53A (v1): SC-5 (1).1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002387 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |
| **Definition:** | The organization defines the denial of service attacks against other information systems that the information system is to restrict the ability of individuals to launch. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SC-5 (1) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001095 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): SC-5 (2)<br>NIST: NIST SP 800-53 Revision 4 (v4): SC-5 (2)<br>NIST: NIST SP 800-53A (v1): SC-5 (2).1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002388 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |
| **Definition:** | The organization defines a list of monitoring tools to be employed to detect indicators of denial of service attacks against the information system. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SC-5 (3) (a) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002389 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |
| **Definition:** | The organization employs an organization-defined list of monitoring tools to detect indicators of denial of service attacks against the information system. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SC-5 (3) (a) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002390 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |
| **Definition:** | The organization defines the information system resources to be monitored to determine if sufficient resources exist to prevent effective denial of service attacks. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SC-5 (3) (b) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002391 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |
| **Definition:** | The organization monitors organization-defined information system resources to determine if sufficient resources exist to prevent effective denial of service attacks. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SC-5 (3) (b) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002392 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published** | 2013-07-02 |

**Date:**

**Definition:** The organization defines the resources to be allocated to protect the availability of information system resources.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-6

---

**CCI:** CCI-002393 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization defines the security safeguards to be employed to protect the availability of information system resources.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-6

---

**CCI:** CCI-002394 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The information system protects the availability of resources by allocating organization-defined resources based on priority, quota, and/or organization-defined security safeguards.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-6

---

**CCI:** CCI-001097 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.

**Type:** policy, technical

**References:** NIST: NIST SP 800-53 (v3): SC-7 a<br>
NIST: NIST SP 800-53 Revision 4 (v4): SC-7 a<br>
NIST: NIST SP 800-53A (v1): SC-7.1 (iii)

---

**CCI:** CCI-002395 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The information system implements subnetworks for publicly accessible system components that are physically and/or logically separated from internal organizational networks.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-7 b

---

**CCI:** CCI-001098 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The information system connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-7 b
NIST: NIST SP 800-53 Revision 4 (v4): SC-7 c
NIST: NIST SP 800-53A (v1): SC-7.1 (iv)

---

**CCI:** CCI-001101 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization limits the number of external network connections to the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-7 (3)
NIST: NIST SP 800-53 Revision 4 (v4): SC-7 (3)
NIST: NIST SP 800-53A (v1): SC-7 (3).1

---

**CCI:** CCI-001102 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization implements a managed interface for each external telecommunication service.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-7 (4) (a)
NIST: NIST SP 800-53 Revision 4 (v4): SC-7 (4) (a)
NIST: NIST SP 800-53A (v1): SC-7 (4).1 (ii)

---

**CCI:** CCI-001103 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization establishes a traffic flow policy for each managed interface for each external telecommunication service.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-7 (4) (b)
NIST: NIST SP 800-53 Revision 4 (v4): SC-7 (4) (b)
NIST: NIST SP 800-53A (v1): SC-7 (4).1 (iii)

---

**CCI:** CCI-002396 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization protects the confidentiality and integrity of the information being transmitted across each interface for each external telecommunication service.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-7 (4) (c)

---

**CCI:** CCI-001105 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need for each external telecommunication service.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): SC-7 (4) (d)
NIST: NIST SP 800-53 Revision 4 (v4): SC-7 (4) (d)
NIST: NIST SP 800-53A (v1): SC-7 (4).1 (v)

---

**CCI:** CCI-001106 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization reviews exceptions to the traffic flow policy on an organization-defined frequency for each external telecommunication service.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): SC-7 (4) (e)
NIST: NIST SP 800-53 Revision 4 (v4): SC-7 (4) (e)
NIST: NIST SP 800-53A (v1): SC-7 (4).1 (vi)

---

**CCI:** CCI-001107 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization defines a frequency for the review of exceptions to the traffic flow policy for each external telecommunication service.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): SC-7 (4) (e)
NIST: NIST SP 800-53 Revision 4 (v4): SC-7 (4) (e)
NIST: NIST SP 800-53A (v1): SC-7 (4).1 (i)

---

**CCI:** CCI-001108 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need for each external telecommunication service.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): SC-7 (4) (f)
NIST: NIST SP 800-53 Revision 4 (v4): SC-7 (4) (e)
NIST: NIST SP 800-53A (v1): SC-7 (4).1 (vii)

---

**CCI:** CCI-001109 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The information system at managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception).

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SC-7 (5)
NIST: NIST SP 800-53 Revision 4 (v4): SC-7 (5)
NIST: NIST SP 800-53A (v1): SC-7 (5).1 (i) (ii)

---

**CCI:** CCI-002397 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The information system, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-7 (7)

---

**CCI:** CCI-001112 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The information system routes organization-defined internal communications traffic to organization-defined external networks through authenticated proxy servers at managed interfaces.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-7 (8)
NIST: NIST SP 800-53 Revision 4 (v4): SC-7 (8)
NIST: NIST SP 800-53A (v1): SC-7 (8).1 (iii)

---

**CCI:** CCI-001113 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization defines the internal communications traffic to be routed to external networks.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-7 (8)
NIST: NIST SP 800-53 Revision 4 (v4): SC-7 (8)
NIST: NIST SP 800-53A (v1): SC-7 (8).1 (i)

---

**CCI:** CCI-001114 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization defines the external networks to which organization-defined internal communications traffic should be routed.

| | | | |
|---|---|---|---|
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SC-7 (8)<br>NIST: NIST SP 800-53 Revision 4 (v4): SC-7 (8)<br>NIST: NIST SP 800-53A (v1): SC-7 (8).1 (ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002398 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |
| **Definition:** | The information system detects outgoing communications traffic posing a threat to external information systems. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SC-7 (9) (a) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002399 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |
| **Definition:** | The information system denies outgoing communications traffic posing a threat to external information systems. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SC-7 (9) (a) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002400 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |
| **Definition:** | The information system audits the identity of internal users associated with denied outgoing communications traffic posing a threat to external information systems. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SC-7 (9) (b) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001116 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization prevents the unauthorized exfiltration of information across managed interfaces. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SC-7 (10)<br>NIST: NIST SP 800-53 Revision 4 (v4): SC-7 (10)<br>NIST: NIST SP 800-53A (v1): SC-7 (10).1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002401 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |
| **Definition:** | The organization defines the authorized sources from which the information system will allow incoming communications. | | |

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-7 (11)

---

**CCI:** CCI-002402 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization defines the authorized destinations for routing inbound communications.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-7 (11)

---

**CCI:** CCI-002403 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The information system only allows incoming communications from organization-defined authorized sources routed to organization-defined authorized destinations.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-7 (11)

---

**CCI:** CCI-002404 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization defines the host-based boundary protection mechanisms that are to be implemented at organization-defined information system components.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-7 (12)

---

**CCI:** CCI-002405 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization defines the information system components at which organization-defined host-based boundary protection mechanisms will be implemented.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-7 (12)

---

**CCI:** CCI-002406 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization implements organization-defined host-based boundary protection mechanisms at organization-defined information system components.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-7 (12)

---

**CCI:** CCI-001119 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization isolates organization-defined information security tools, mechanisms, and support components from other internal information system components by implementing physically separate subnetworks with managed interfaces to other components of the system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-7 (13)
NIST: NIST SP 800-53 Revision 4 (v4): SC-7 (13)
NIST: NIST SP 800-53A (v1): SC-7 (13).1 (ii)

---

**CCI:** CCI-001120 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization defines key information security tools, mechanisms, and support components to be isolated.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-7 (13)
NIST: NIST SP 800-53 Revision 4 (v4): SC-7 (13)
NIST: NIST SP 800-53A (v1): SC-7 (13).1 (iii)

---

**CCI:** CCI-001121 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization protects against unauthorized physical connections at organization-defined managed interfaces.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-7 (14)
NIST: NIST SP 800-53 Revision 4 (v4): SC-7 (14)
NIST: NIST SP 800-53A (v1): SC-7 (14).1 (iii)

---

**CCI:** CCI-001122 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization defines the managed interfaces where boundary protections against unauthorized physical connections are to be implemented.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-7 (14)
NIST: NIST SP 800-53 Revision 4 (v4): SC-7 (14)
NIST: NIST SP 800-53A (v1): SC-7 (14).1 (i)

---

**CCI:** CCI-002407 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization defines the managed interfaces at which the organization protects against unauthorized physical connections.

| | | | |
|---|---|---|---|
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SC-7 (14) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001123 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The information system routes all networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing. | | |
| **Type:** | policy, technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): SC-7 (15)<br>NIST: NIST SP 800-53 Revision 4 (v4): SC-7 (15)<br>NIST: NIST SP 800-53A (v1): SC-7 (15).1 (i) (ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001124 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The information system prevents discovery of specific system components composing a managed interface. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): SC-7 (16)<br>NIST: NIST SP 800-53 Revision 4 (v4): SC-7 (16)<br>NIST: NIST SP 800-53A (v1): SC-7 (16).1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001125 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The information system enforces adherence to protocol format. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): SC-7 (17)<br>NIST: NIST SP 800-53 Revision 4 (v4): SC-7 (17)<br>NIST: NIST SP 800-53A (v1): SC-7 (17).1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001126 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The information system fails securely in the event of an operational failure of a boundary protection device. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): SC-7 (18)<br>NIST: NIST SP 800-53 Revision 4 (v4): SC-7 (18)<br>NIST: NIST SP 800-53A (v1): SC-7 (18) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002408 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published** | 2013-07-02 |

**Date:**

**Definition:** The organization defines the independently configured communication clients, which are configured by end users and external service providers, between which the information system will block both inbound and outbound communications traffic.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-7 (19)

---

**CCI:** CCI-002409 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The information system blocks both inbound and outbound communications traffic between organization-defined communication clients that are independently configured by end users and external service providers.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-7 (19)

---

**CCI:** CCI-002410 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization defines information system components that are to be dynamically isolated/segregated from other components of the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-7 (20)

---

**CCI:** CCI-002411 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The information system provides the capability to dynamically isolate/segregate organization-defined information system components from other components of the system.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-7 (20)

---

**CCI:** CCI-002412 **Status:** deprecated

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization defines the information system components supporting organization-defined missions and/or business functions that are to be separated using boundary protection mechanisms.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-7 (21)

---

**CCI:** CCI-002413 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization defines the information system components supporting organization-defined missions and/or business functions that are to be separated using boundary protection mechanisms.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-7 (21)

---

**CCI:** CCI-002414 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization defines the missions and/or business functions for which boundary protection mechanisms will be employed to separate the supporting organization-defined information system components.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-7 (21)

---

**CCI:** CCI-002415 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization employs boundary protection mechanisms to separate organization-defined information system components supporting organization-defined missions and/or business functions.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-7 (21)

---

**CCI:** CCI-002416 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The information system implements separate network addresses (i.e., different subnets) to connect to systems in different security domains.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-7 (22)

---

**CCI:** CCI-002417 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The information system disables feedback to senders on protocol format validation failure.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-7 (23)

---

**CCI:** CCI-002418 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The information system protects the confidentiality and/or integrity of transmitted information.

**Type:** policy, technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-8

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002419 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |
| **Definition:** | The organization defines the alternative physical safeguards to be employed when cryptographic mechanisms are not implemented to protect information during transmission. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SC-8 (1) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002421 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |
| **Definition:** | The information system implements cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission unless otherwise protected by organization-defined alternative physical safeguards. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SC-8 (1) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002420 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |
| **Definition:** | The information system maintains the confidentiality and/or integrity of information during preparation for transmission. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SC-8 (2) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002422 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |
| **Definition:** | The information system maintains the confidentiality and/or integrity of information during reception. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SC-8 (2) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002423 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |
| **Definition:** | The information system implements cryptographic mechanisms to protect message externals (e.g., message headers and routing information) unless otherwise protected by organization-defined alternative physical safeguards. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SC-8 (3) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002427 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published** | 2013-07-02 |

**Date:**

**Definition:** The organization defines the alternative physical safeguards to be employed to protect message externals (e.g., message headers and routing information) when cryptographic mechanisms are not implemented.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-8 (3)

---

**CCI:** CCI-002424 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization defines the alternative physical safeguards to be employed when cryptographic mechanisms are not implemented by the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-8 (4)

---

**CCI:** CCI-002425 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The information system implements cryptographic mechanisms to conceal or randomize communication patterns unless otherwise protected by organization-defined alternative physical safeguards.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-8 (4)

---

**CCI:** CCI-001133 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The information system terminates the network connection associated with a communications session at the end of the session or after an organization-defined time period of inactivity.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SC-10
NIST: NIST SP 800-53 Revision 4 (v4): SC-10
NIST: NIST SP 800-53A (v1): SC-10.1 (ii)

---

**CCI:** CCI-001134 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization defines the time period of inactivity after which the information system terminates a network connection associated with a communications session.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-10
NIST: NIST SP 800-53 Revision 4 (v4): SC-10
NIST: NIST SP 800-53A (v1): SC-10.1 (i)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001661 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-12 |
| **Definition:** | The organization defines the security functions, to minimally include information system authentication and re-authentication, within the information system to be included in a trusted communications path. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SC-11<br>NIST: NIST SP 800-53 Revision 4 (v4): SC-11<br>NIST: NIST SP 800-53A (v1): SC-11.1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001135 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The information system establishes a trusted communications path between the user and organization-defined security functions within the information system. | | |
| **Type:** | policy, technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): SC-11<br>NIST: NIST SP 800-53 Revision 4 (v4): SC-11<br>NIST: NIST SP 800-53A (v1): SC-11.1 (iii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002426 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |
| **Definition:** | The information system provides a trusted communications path that is logically isolated and distinguishable from other paths. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SC-11 (1) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002428 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |
| **Definition:** | The organization defines the requirements for cryptographic key generation to be employed within the information system. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SC-12 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002429 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |
| **Definition:** | The organization defines the requirements for cryptographic key distribution to be employed within the information system. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SC-12 | | |

**CCI:** CCI-002430 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-07-02
**Definition:** The organization defines the requirements for cryptographic key storage to be employed within the information system.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-12

---

**CCI:** CCI-002431 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-07-02
**Definition:** The organization defines the requirements for cryptographic key access to be employed within the information system.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-12

---

**CCI:** CCI-002432 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-07-02
**Definition:** The organization defines the requirements for cryptographic key destruction to be employed within the information system.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-12

---

**CCI:** CCI-002433 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-07-02
**Definition:** The organization establishes cryptographic keys for required cryptography employed within the information system in accordance with organization-defined requirements for key generation.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-12

---

**CCI:** CCI-002434 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-07-02
**Definition:** The organization establishes cryptographic keys for required cryptography employed within the information system in accordance with organization-defined requirements for key distribution.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-12

---

**CCI:** CCI-002435 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization establishes cryptographic keys for required cryptography employed within the information system in accordance with organization-defined requirements for key storage.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-12

---

**CCI:** CCI-002436 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization establishes cryptographic keys for required cryptography employed within the information system in accordance with organization-defined requirements for key access.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-12

---

**CCI:** CCI-002437 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization establishes cryptographic keys for required cryptography employed within the information system in accordance with organization-defined requirements for key destruction.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-12

---

**CCI:** CCI-002438 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization manages cryptographic keys for required cryptography employed within the information system in accordance with organization-defined requirements for key generation.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-12

---

**CCI:** CCI-002439 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization manages cryptographic keys for required cryptography employed within the information system in accordance with organization-defined requirements for key distribution.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-12

---

**CCI:** CCI-002440 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization manages cryptographic keys for required cryptography employed within the information system in accordance with organization-defined requirements for key storage.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-12

---

**CCI:** CCI-002441 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization manages cryptographic keys for required cryptography employed within the information system in accordance with organization-defined requirements for key access.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-12

---

**CCI:** CCI-002442 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization manages cryptographic keys for required cryptography employed within the information system in accordance with organization-defined requirements for key destruction.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-12

---

**CCI:** CCI-001139 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization maintains availability of information in the event of the loss of cryptographic keys by users.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-12 (1)
NIST: NIST SP 800-53 Revision 4 (v4): SC-12 (1)
NIST: NIST SP 800-53A (v1): SC-12 (1).1

---

**CCI:** CCI-002443 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization produces symmetric cryptographic keys using NIST FIPS-compliant or NSA-approved key management technology and processes.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-12 (2)

---

**CCI:** CCI-002444 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization controls symmetric cryptographic keys using NIST FIPS-compliant or NSA-approved key management technology and processes.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-12 (2)

---

**CCI:** CCI-002445 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization distributes symmetric cryptographic keys using NIST FIPS-compliant or NSA-approved key management technology and processes.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-12 (2)

---

**CCI:** CCI-002446 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization produces asymmetric cryptographic keys using: NSA-approved key management technology and processes; approved PKI Class 3 certificates or prepositioned keying material; or approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user's private key.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-12 (3)

---

**CCI:** CCI-002447 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization controls asymmetric cryptographic keys using: NSA-approved key management technology and processes; approved PKI Class 3 certificates or prepositioned keying material; or approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user's private key.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-12 (3)

---

**CCI:** CCI-002448 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization distributes asymmetric cryptographic keys using: NSA-approved key management technology and processes; approved PKI Class 3 certificates or prepositioned keying material; or approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user's private key.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-12 (3)

---

**CCI:** CCI-002449 **Status:** draft

**Contributor:** DISA FSO **Published** 2013-07-02

**Date:**

**Definition:** The organization defines the cryptographic uses, and type of cryptography required for each use, to be implemented by the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-13

---

**CCI:** CCI-002450
**Status:** draft

**Contributor:** DISA FSO
**Published Date:** 2013-07-02

**Definition:** The information system implements organization-defined cryptographic uses and type of cryptography required for each use in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-13

---

**CCI:** CCI-001150
**Status:** draft

**Contributor:** DISA FSO
**Published Date:** 2009-09-21

**Definition:** The information system prohibits remote activation of collaborative computing devices, excluding the organization-defined exceptions where remote activation is to be allowed.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SC-15 a
NIST: NIST SP 800-53 Revision 4 (v4): SC-15 a
NIST: NIST SP 800-53A (v1): SC-15.1 (ii)

---

**CCI:** CCI-001151
**Status:** draft

**Contributor:** DISA FSO
**Published Date:** 2009-09-21

**Definition:** The organization defines exceptions to the prohibition of collaborative computing devices where remote activation is to be allowed.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-15 a
NIST: NIST SP 800-53 Revision 4 (v4): SC-15 a
NIST: NIST SP 800-53A (v1): SC-15.1 (i)

---

**CCI:** CCI-001152
**Status:** draft

**Contributor:** DISA FSO
**Published Date:** 2009-09-21

**Definition:** The information system provides an explicit indication of use to users physically present at collaborative computing devices.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SC-15 b
NIST: NIST SP 800-53 Revision 4 (v4): SC-15 b
NIST: NIST SP 800-53A (v1): SC-15.1 (iii)

---

**CCI:** CCI-001153 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The information system provides physical disconnect of collaborative computing devices in a manner that supports ease of use.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SC-15 (1)

NIST: NIST SP 800-53 Revision 4 (v4): SC-15 (1)

NIST: NIST SP 800-53A (v1): SC-15 (1).1

---

**CCI:** CCI-001155 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization disables or removes collaborative computing devices from organization-defined information systems or information system components in organization-defined secure work areas.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-15 (3)

NIST: NIST SP 800-53 Revision 4 (v4): SC-15 (3)

NIST: NIST SP 800-53A (v1): SC-15 (3).1 (ii)

---

**CCI:** CCI-001156 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization defines secure work areas where collaborative computing devices are to be disabled or removed.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-15 (3)

NIST: NIST SP 800-53 Revision 4 (v4): SC-15 (3)

NIST: NIST SP 800-53A (v1): SC-15 (3).1 (i)

---

**CCI:** CCI-002451 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization defines the information systems or information system components from which collaborative computing devices in organization-defined secure work areas are to be disabled or removed.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-15 (3)

---

**CCI:** CCI-002452 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization defines the online meetings and teleconferences for which the information system provides an explicit indication of current participants.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-15 (4)

---

**CCI:** CCI-002453 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The information system provides an explicit indication of current participants in organization-defined online meetings and teleconferences.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-15 (4)

---

**CCI:** CCI-001157 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The information system associates organization-defined security attributes with information exchanged between information systems.

**Type:** policy, technical

**References:** NIST: NIST SP 800-53 (v3): SC-16

NIST: NIST SP 800-53 Revision 4 (v4): SC-16

NIST: NIST SP 800-53A (v1): SC-16.1

---

**CCI:** CCI-002454 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization defines the security attributes the information system is to associate with the information being exchanged between information systems and between information system components.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-16

---

**CCI:** CCI-002455 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The information system associates organization-defined security attributes with information exchanged between information system components.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-16

---

**CCI:** CCI-001158 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The information system validates the integrity of transmitted security attributes.

**Type:** technical

| | | | |
|---|---|---|---|
| **References:** | NIST: NIST SP 800-53 (v3): SC-16 (1)<br>NIST: NIST SP 800-53 Revision 4 (v4): SC-16 (1)<br>NIST: NIST SP 800-53A (v1): SC-16 (1).1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001159 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization issues public key certificates under an organization-defined certificate policy or obtains public key certificates from an approved service provider. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SC-17<br>NIST: NIST SP 800-53 Revision 4 (v4): SC-17<br>NIST: NIST SP 800-53A (v1): SC-17.1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002456 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |
| **Definition:** | The organization defines the certificate policy employed to issue public key certificates. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SC-17 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001160 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization defines acceptable and unacceptable mobile code and mobile code technologies. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SC-18 a<br>NIST: NIST SP 800-53 Revision 4 (v4): SC-18 a<br>NIST: NIST SP 800-53A (v1): SC-18.1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001162 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization establishes implementation guidance for acceptable mobile code and mobile code technologies. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SC-18 b<br>NIST: NIST SP 800-53 Revision 4 (v4): SC-18 b<br>NIST: NIST SP 800-53A (v1): SC-18.1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001161 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |

**Definition:** The organization establishes usage restrictions for acceptable mobile code and mobile code technologies.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-18 b
NIST: NIST SP 800-53 Revision 4 (v4): SC-18 b
NIST: NIST SP 800-53A (v1): SC-18.1 (ii)

---

**CCI:** CCI-001163 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization authorizes the use of mobile code within the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-18 c
NIST: NIST SP 800-53 Revision 4 (v4): SC-18 c
NIST: NIST SP 800-53A (v1): SC-18.1 (iii)

---

**CCI:** CCI-001164 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization monitors the use of mobile code within the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-18 c
NIST: NIST SP 800-53 Revision 4 (v4): SC-18 c
NIST: NIST SP 800-53A (v1): SC-18.1 (iii)

---

**CCI:** CCI-001165 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization controls the use of mobile code within the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-18 c
NIST: NIST SP 800-53 Revision 4 (v4): SC-18 c
NIST: NIST SP 800-53A (v1): SC-18.1 (iii)

---

**CCI:** CCI-001662 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2010-05-12

**Definition:** The information system takes organization-defined corrective action when organization-defined unacceptable mobile code is identified.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SC-18 (1)
NIST: NIST SP 800-53 Revision 4 (v4): SC-18 (1)
NIST: NIST SP 800-53A (v1): SC-18 (1).1 (ii)

---

**CCI:** CCI-001166 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The information system identifies organization-defined unacceptable mobile code.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SC-18 (1)
NIST: NIST SP 800-53 Revision 4 (v4): SC-18 (1)
NIST: NIST SP 800-53A (v1): SC-18 (1).1 (i)

---

**CCI:** CCI-002457 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization defines the corrective actions to be taken when organization-defined unacceptable mobile code is identified.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-18 (1)

---

**CCI:** CCI-002458 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization defines what constitutes unacceptable mobile code for its information systems.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-18 (1)

---

**CCI:** CCI-001167 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization ensures the development of mobile code to be deployed in information systems meets organization-defined mobile code requirements.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-18 (2)
NIST: NIST SP 800-53 Revision 4 (v4): SC-18 (2)
NIST: NIST SP 800-53A (v1): SC-18 (2).1 (ii)

---

**CCI:** CCI-001168 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization defines requirements for the acquisition, development, and use of mobile code.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-18 (2)
NIST: NIST SP 800-53 Revision 4 (v4): SC-18 (2)
NIST: NIST SP 800-53A (v1): SC-18 (2).1 (i)

---

**CCI:** CCI-001687
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2011-05-03
**Definition:** The organization ensures the use of mobile code to be deployed in information systems meets organization-defined mobile code requirements.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): SC-18 (2)
NIST: NIST SP 800-53 Revision 4 (v4): SC-18 (2)
NIST: NIST SP 800-53A (v1): SC-18 (2).1 (ii)

---

**CCI:** CCI-001688
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2011-05-03
**Definition:** The organization ensures the acquisition of mobile code to be deployed in information systems meets organization-defined mobile code requirements.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): SC-18 (2)
NIST: NIST SP 800-53 Revision 4 (v4): SC-18 (2)
NIST: NIST SP 800-53A (v1): SC-18 (2).1 (ii)

---

**CCI:** CCI-001169
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2009-09-21
**Definition:** The information system prevents the download of organization-defined unacceptable mobile code.
**Type:** technical
**References:** NIST: NIST SP 800-53 (v3): SC-18 (3)
NIST: NIST SP 800-53 Revision 4 (v4): SC-18 (3)
NIST: NIST SP 800-53A (v1): SC-18 (3).1

---

**CCI:** CCI-001695
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2011-10-07
**Definition:** The information system prevents the execution of organization-defined unacceptable mobile code.
**Type:** technical
**References:** NIST: NIST SP 800-53 (v3): SC-18 (3)
NIST: NIST SP 800-53 Revision 4 (v4): SC-18 (3)
NIST: NIST SP 800-53A (v1): SC-18 (3).1

---

**CCI:** CCI-002459
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2013-07-02
**Definition:** The organization defines the unacceptable mobile code of which the information system is

to prevent download and execution.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-18 (3)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001170 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |

**Definition:** The information system prevents the automatic execution of mobile code in organization-defined software applications.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SC-18 (4)
NIST: NIST SP 800-53 Revision 4 (v4): SC-18 (4)
NIST: NIST SP 800-53A (v1): SC-18 (4).1 (iii) (iv)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001171 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |

**Definition:** The organization defines software applications in which automatic mobile code execution is to be prohibited.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-18 (4)
NIST: NIST SP 800-53 Revision 4 (v4): SC-18 (4)
NIST: NIST SP 800-53A (v1): SC-18 (4).1 (i)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001172 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |

**Definition:** The organization defines actions to be enforced by the information system before executing mobile code.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-18 (4)
NIST: NIST SP 800-53 Revision 4 (v4): SC-18 (4)
NIST: NIST SP 800-53A (v1): SC-18 (4).1 (ii)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002460 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |

**Definition:** The information system enforces organization-defined actions prior to executing mobile code.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-18 (4)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002461 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published** | 2013-07-02 |

**Date:**

**Definition:** The organization allows execution of permitted mobile code only in confined virtual machine environments.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-18 (5)

---

**CCI:** CCI-001173 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization establishes usage restrictions for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-19 a
NIST: NIST SP 800-53 Revision 4 (v4): SC-19 a
NIST: NIST SP 800-53A (v1): SC-19.1 (i)

---

**CCI:** CCI-001174 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization establishes implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-19 a
NIST: NIST SP 800-53 Revision 4 (v4): SC-19 a
NIST: NIST SP 800-53A (v1): SC-19.1 (i)

---

**CCI:** CCI-001175 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization authorizes the use of VoIP within the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-19 b
NIST: NIST SP 800-53 Revision 4 (v4): SC-19 b
NIST: NIST SP 800-53A (v1): SC-19.1 (ii)

---

**CCI:** CCI-001176 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization monitors the use of VoIP within the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-19 b
NIST: NIST SP 800-53 Revision 4 (v4): SC-19 b

NIST: NIST SP 800-53A (v1): SC-19.1 (ii)

---

**CCI:** CCI-001177 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization controls the use of VoIP within the information system.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): SC-19 b
NIST: NIST SP 800-53 Revision 4 (v4): SC-19 b
NIST: NIST SP 800-53A (v1): SC-19.1 (ii)

---

**CCI:** CCI-001178 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The information system provides additional data origin authentication artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries.
**Type:** technical
**References:** NIST: NIST SP 800-53 (v3): SC-20
NIST: NIST SP 800-53 Revision 4 (v4): SC-20 a
NIST: NIST SP 800-53A (v1): SC-20.1

---

**CCI:** CCI-002462 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-07-02
**Definition:** The information system provides additional data integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries.
**Type:** technical
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-20 a

---

**CCI:** CCI-001663 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2010-05-12
**Definition:** The information system, when operating as part of a distributed, hierarchical namespace, provides the means to enable verification of a chain of trust among parent and child domains (if the child supports secure resolution services).
**Type:** technical
**References:** NIST: NIST SP 800-53 (v3): SC-20 (1)
NIST: NIST SP 800-53 Revision 4 (v4): SC-20 b
NIST: NIST SP 800-53A (v1): SC-20 (1).1 (ii)

---

**CCI:** CCI-001179 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child zones.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SC-20 (1)<br>NIST: NIST SP 800-53 Revision 4 (v4): SC-20 b<br>NIST: NIST SP 800-53A (v1): SC-20 (1).1 (i)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002463 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |

**Definition:** The information system provides data origin artifacts for internal name/address resolution queries.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-20 (2)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002464 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |

**Definition:** The information system provides data integrity protection artifacts for internal name/address resolution queries.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-20 (2)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002465 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |

**Definition:** The information system requests data origin authentication verification on the name/address resolution responses the system receives from authoritative sources.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-21

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002466 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |

**Definition:** The information system requests data integrity verification on the name/address resolution responses the system receives from authoritative sources.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-21

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002467 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |

**Definition:** The information system performs data integrity verification on the name/address resolution responses the system receives from authoritative sources.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-21

---

**CCI:** CCI-002468 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The information system performs data origin verification authentication on the name/address resolution responses the system receives from authoritative sources.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-21

---

**CCI:** CCI-001182 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The information systems that collectively provide name/address resolution service for an organization are fault-tolerant.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-22
NIST: NIST SP 800-53 Revision 4 (v4): SC-22
NIST: NIST SP 800-53A (v1): SC-22.1 (i)

---

**CCI:** CCI-001183 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The information systems that collectively provide name/address resolution service for an organization implement internal/external role separation.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-22
NIST: NIST SP 800-53 Revision 4 (v4): SC-22
NIST: NIST SP 800-53A (v1): SC-22.1 (ii)

---

**CCI:** CCI-001184 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The information system protects the authenticity of communications sessions.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SC-23
NIST: NIST SP 800-53 Revision 4 (v4): SC-23
NIST: NIST SP 800-53A (v1): SC-23.1

---

**CCI:** CCI-001185 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The information system invalidates session identifiers upon user logout or other session

| | |
|---|---|
| | termination. |
| **Type:** | technical |
| **References:** | NIST: NIST SP 800-53 (v3): SC-23 (1)<br>NIST: NIST SP 800-53 Revision 4 (v4): SC-23 (1)<br>NIST: NIST SP 800-53A (v1): SC-23 (1).1 |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001664 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-12 |
| **Definition:** | The information system recognizes only session identifiers that are system-generated. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): SC-23 (3)<br>NIST: NIST SP 800-53 Revision 4 (v4): SC-23 (3)<br>NIST: NIST SP 800-53A (v1): SC-23 (3).1 (ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001188 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The information system generates unique session identifiers for each session with organization-defined randomness requirements. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): SC-23 (4)<br>NIST: NIST SP 800-53 Revision 4 (v4): SC-23 (3)<br>NIST: NIST SP 800-53A (v1): SC-23 (4).1 (ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001189 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization defines randomness requirements for generating unique session identifiers. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SC-23 (4)<br>NIST: NIST SP 800-53 Revision 4 (v4): SC-23 (3)<br>NIST: NIST SP 800-53A (v1): SC-23 (4).1 (i) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002469 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |
| **Definition:** | The organization defines the certificate authorities the information system will allow to be used on the information system. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SC-23 (5) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002470 | **Status:** | draft |

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The information system only allows the use of organization-defined certificate authorities for verification of the establishment of protected sessions.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-23 (5)

---

**CCI:** CCI-001665 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2010-05-12

**Definition:** The information system preserves organization-defined system state information in the event of a system failure.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SC-24

NIST: NIST SP 800-53 Revision 4 (v4): SC-24

NIST: NIST SP 800-53A (v1): SC-24.1 (v)

---

**CCI:** CCI-001190 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The information system fails to an organization-defined known-state for organization-defined types of failures.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SC-24

NIST: NIST SP 800-53 Revision 4 (v4): SC-24

NIST: NIST SP 800-53A (v1): SC-24.1 (iv)

---

**CCI:** CCI-001191 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization defines the known states the information system should fail to in the event of an organization-defined system failure.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-24

NIST: NIST SP 800-53 Revision 4 (v4): SC-24

NIST: NIST SP 800-53A (v1): SC-24.1 (i)

---

**CCI:** CCI-001192 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization defines types of failures for which the information system should fail to an organization-defined known state.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-24

| | | | |
|---|---|---|---|
| | NIST: NIST SP 800-53 Revision 4 (v4): SC-24<br>NIST: NIST SP 800-53A (v1): SC-24.1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001193 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization defines system state information that should be preserved in the event of a system failure. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SC-24<br>NIST: NIST SP 800-53 Revision 4 (v4): SC-24<br>NIST: NIST SP 800-53A (v1): SC-24.1 (iii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001194 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The information system employs organization-defined information system components with minimal functionality and information storage. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SC-25<br>NIST: NIST SP 800-53 Revision 4 (v4): SC-25<br>NIST: NIST SP 800-53A (v1): SC-25.1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002471 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |
| **Definition:** | The organization defines the information system components, with minimal functionality and information storage, to be employed. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SC-25 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001195 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The information system includes components specifically designed to be the target of malicious attacks for the purpose of detecting, deflecting, and analyzing such attacks. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SC-26<br>NIST: NIST SP 800-53 Revision 4 (v4): SC-26<br>NIST: NIST SP 800-53A (v1): SC-26.1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001197 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |

**Definition:** The information system includes organization-defined platform-independent applications.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-27
NIST: NIST SP 800-53 Revision 4 (v4): SC-27
NIST: NIST SP 800-53A (v1): SC-27.1 (ii)

---

**CCI:** CCI-001198 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization defines applications that are platform independent.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-27
NIST: NIST SP 800-53 Revision 4 (v4): SC-27
NIST: NIST SP 800-53A (v1): SC-27.1 (i)

---

**CCI:** CCI-001199 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The information system protects the confidentiality and/or integrity of organization-defined information at rest.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SC-28
NIST: NIST SP 800-53 Revision 4 (v4): SC-28
NIST: NIST SP 800-53A (v1): SC-28.1

---

**CCI:** CCI-002472 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization defines the information at rest that is to be protected by the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-28

---

**CCI:** CCI-002473 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization defines the information at rest for which cryptographic mechanisms will be implemented.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-28 (1)

---

**CCI:** CCI-002474 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization defines the information system components which require the implementation of cryptographic mechanisms to prevent unauthorized disclosure and modification of organization-defined information at rest.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-28 (1)

---

**CCI:** CCI-002475 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The information system implements cryptographic mechanisms to prevent unauthorized modification of organization-defined information at rest on organization-defined information system components.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-28 (1)

---

**CCI:** CCI-002476 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The information system implements cryptographic mechanisms to prevent unauthorized disclosure of organization-defined information at rest on organization-defined information system components.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-28 (1)

---

**CCI:** CCI-002477 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization defines the information at rest to be removed from online storage and stored in an off-line secure location.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-28 (2)

---

**CCI:** CCI-002478 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization removes organization-defined information at rest from online storage.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-28 (2)

---

**CCI:** CCI-002479 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization stores organization-defined information at rest in an off-line secure location.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-28 (2)

---

**CCI:** CCI-001201 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization employs a diverse set of information technologies for organization-defined information system components in the implementation of the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-29

NIST: NIST SP 800-53 Revision 4 (v4): SC-29

NIST: NIST SP 800-53A (v1): SC-29.1

---

**CCI:** CCI-002480 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization defines the information system components for which a diverse set of information technologies are to be employed.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-29

---

**CCI:** CCI-001203 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization employs virtualization techniques to support the deployment of a diversity of operating systems that are changed on an organization-defined frequency.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-30 (1)

NIST: NIST SP 800-53 Revision 4 (v4): SC-29 (1)

NIST: NIST SP 800-53A (v1): SC-30 (1).1 (ii)

---

**CCI:** CCI-001204 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization defines the frequency of changes to operating systems and applications to support a diversity of deployments.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-30 (1)

NIST: NIST SP 800-53 Revision 4 (v4): SC-29 (1)

NIST: NIST SP 800-53A (v1): SC-30 (1).1 (i)

---

**CCI:** CCI-002481 **Status:** draft

**Contributor:** DISA FSP **Published Date:** 2013-07-02

**Definition:** The organization employs virtualization techniques to support the deployment of a diversity of applications that are changed per organization-defined frequency.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-29 (1)

---

**CCI:** CCI-002482 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization defines the concealment and misdirection techniques employed for organization-defined information systems to confuse and mislead adversaries.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-30

---

**CCI:** CCI-002483 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization defines the information systems for which organization-defined concealment and misdirection techniques are to be employed.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-30

---

**CCI:** CCI-002484 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization defines the time periods at which it will employ organization-defined concealment and misdirection techniques on organization-defined information systems.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-30

---

**CCI:** CCI-002485 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization employs organization-defined concealment and misdirection techniques for organization-defined information systems at organization-defined time periods to confuse and mislead adversaries.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-30

---

**CCI:** CCI-002486 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization defines the techniques to be employed to introduce randomness into organizational operations and assets.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-30 (2)

---

**CCI:** CCI-002487
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2013-07-02
**Definition:** The organization employs organization-defined techniques to introduce randomness into organizational operations.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-30 (2)

---

**CCI:** CCI-002488
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2013-07-02
**Definition:** The organization employs organization-defined techniques to introduce randomness into organizational assets.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-30 (2)

---

**CCI:** CCI-002489
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2013-07-02
**Definition:** The organization defines the processing and/or storage locations to be changed at random intervals or at an organization-defined frequency.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-30 (3)

---

**CCI:** CCI-002490
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2013-07-02
**Definition:** The organization defines the frequency at which it changes the location of organization-defined processing and/or storage.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-30 (3)

---

**CCI:** CCI-002491
**Status:** deprecated
**Contributor:** DISA FSO
**Published Date:** 2013-07-02
**Definition:** The organization changes the location of organization-defined processing and/or storage at an organization-defined time frequency or at random time intervals.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-30 (3)

---

**CCI:** CCI-002492
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2013-07-02
**Definition:** The organization changes the location of organization-defined processing and/or storage at an organization-defined time frequency or at random time intervals.

| | | | |
|---|---|---|---|
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SC-30 (3) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002493 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |
| **Definition:** | The organization defines the information system components in which it will employ realistic but misleading information regarding its security state or posture. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SC-30 (4) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002494 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |
| **Definition:** | The organization employs realistic, but misleading, information in organization-defined information system components with regard to its security state or posture. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SC-30 (4) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002495 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |
| **Definition:** | The organization defines the techniques to be employed to hide or conceal organization-defined information system components. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SC-30 (5) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002496 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |
| **Definition:** | The organization defines the information system components to be hidden or concealed. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SC-30 (5) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002497 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |
| **Definition:** | The organization employs organization-defined techniques to hide or conceal organization-defined information system components. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SC-30 (5) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002498 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |

**Definition:** The organization performs a covert channel analysis to identify those aspects of communications within the information system that are potential avenues for covert storage and/or timing channels.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-31 a

---

**CCI:** CCI-002499 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization estimates the maximum bandwidth of the covert storage and timing channels.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-31 b

---

**CCI:** CCI-001207 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization tests a subset of the identified covert channels to determine which channels are exploitable.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-31 (1)
NIST: NIST SP 800-53 Revision 4 (v4): SC-31 (1)
NIST: NIST SP 800-53A (v1): SC-31 (1).1

---

**CCI:** CCI-002500 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization defines the maximum bandwidth values to which covert storage and/or timing channels are to be reduced.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-31 (2)

---

**CCI:** CCI-002501 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization reduces the maximum bandwidth for identified covert storage and/or timing channels to organization-defined values.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-31 (2)

---

**CCI:** CCI-002502 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization defines the subset of identified covert channels in the operational environment of the information system that are to have the bandwidth measured.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-31 (3)

---

**CCI:** CCI-002503 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization measures the bandwidth of an organization-defined subset of identified covert channels in the operational environment of the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-31 (3)

---

**CCI:** CCI-002504 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization defines the information system components into which the information system is partitioned.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-32

---

**CCI:** CCI-002505 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization defines the circumstances under which the information system components are to be physically separated to support partitioning.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-32

---

**CCI:** CCI-002506 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization partitions the information system into organization-defined information system components residing in separate physical domains or environments based on organization-defined circumstances for physical separation of components.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-32

---

**CCI:** CCI-001212 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization defines information system components on which the operating environment and organization-defined applications are loaded and executed from hardware-enforced, read-only media.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-34
NIST: NIST SP 800-53 Revision 4 (v4): SC-34

NIST: NIST SP 800-53A (v1): SC-34.1 (ii)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001210 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |

**Definition:** The information system, at organization-defined information system components, loads and executes the operating environment from hardware-enforced, read-only media.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SC-34 a
NIST: NIST SP 800-53 Revision 4 (v4): SC-34 a
NIST: NIST SP 800-53A (v1): SC-34.1 (iii)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001211 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |

**Definition:** The information system, at organization-defined information system components, loads and executes organization-defined applications from hardware-enforced, read-only media.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SC-34 b
NIST: NIST SP 800-53 Revision 4 (v4): SC-34 b
NIST: NIST SP 800-53A (v1): SC-34.1 (iii)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001213 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |

**Definition:** The organization defines applications that will be loaded and executed from hardware-enforced, read-only media.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-34 b
NIST: NIST SP 800-53 Revision 4 (v4): SC-34 b
NIST: NIST SP 800-53A (v1): SC-34.1 (i)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001214 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |

**Definition:** The organization employs organization-defined information system components with no writeable storage that are persistent across component restart or power on/off.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-34 (1)
NIST: NIST SP 800-53 Revision 4 (v4): SC-34 (1)
NIST: NIST SP 800-53A (v1): SC-34 (1).1 (ii)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001215 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published** | 2009-09-21 |

| | | | |
|---|---|---|---|
| | | **Date:** | |
| **Definition:** | The organization defines the information system components to be employed with no writeable storage. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SC-34 (1)<br>NIST: NIST SP 800-53 Revision 4 (v4): SC-34 (1)<br>NIST: NIST SP 800-53A (v1): SC-34 (1).1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001216 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization protects the integrity of information prior to storage on read-only media. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SC-34 (2)<br>NIST: NIST SP 800-53 Revision 4 (v4): SC-34 (2)<br>NIST: NIST SP 800-53A (v1): SC-34 (2).1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002507 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |
| **Definition:** | The organization controls read-only media after information has been recorded onto the media. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SC-34 (2) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002508 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |
| **Definition:** | The organization defines the information system firmware components for which hardware-based, write-protect is employed. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SC-34 (3) (a) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002509 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |
| **Definition:** | The organization employs hardware-based, write-protect for organization-defined information system firmware components. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SC-34 (3) (a) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002510 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |

**Definition:** The organization defines the individuals authorized to manually disable hardware-based, write-protect for firmware modifications and re-enable the write-protect prior to returning to operational mode.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-34 (3) (b)

---

**CCI:** CCI-002511 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization implements specific procedures for organization-defined authorized individuals to manually disable hardware-based, write-protect for firmware modifications.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-34 (3) (b)

---

**CCI:** CCI-002512 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization implements specific procedures for organization-defined authorized individuals to manually re-enable hardware write-protect prior to returning to operational mode.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-34 (3) (b)

---

**CCI:** CCI-001196 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The information system includes components that proactively seek to identify malicious websites and/or web-based malicious code.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-26 (1)
NIST: NIST SP 800-53 Revision 4 (v4): SC-35
NIST: NIST SP 800-53A (v1): SC-26 (1).1

---

**CCI:** CCI-002513 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization defines the processing that is to be distributed across multiple physical locations.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-36

---

**CCI:** CCI-002514 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization defines the storage that is to be distributed across multiple physical locations.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-36

---

**CCI:** CCI-002515 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization distributes organization-defined processing across multiple physical locations.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-36

---

**CCI:** CCI-002516 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization distributes organization-defined storage across multiple physical locations.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-36

---

**CCI:** CCI-002517 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization defines the distributed processing components that are to be polled to identify potential faults, errors, or compromises.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-36 (1)

---

**CCI:** CCI-002518 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization defines the distributed storage components that are to be polled to identify potential faults, errors, or compromises.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-36 (1)

---

**CCI:** CCI-002519 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization employs polling techniques to identify potential faults, errors, or compromises to organization-defined distributed processing components.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-36 (1)

---

**CCI:** CCI-002520 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization employs polling techniques to identify potential faults, errors, or compromises to organization-defined distributed storage components.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-36 (1)

---

**CCI:** CCI-002521 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization defines the out-of-band channels to be employed for the physical delivery or electronic transmission of organization-defined information, information system components, or devices.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-37

---

**CCI:** CCI-002522 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization defines the information, information system components, or devices that are to be electronically transmitted or physically delivered via organization-defined out-of-band channels.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-37

---

**CCI:** CCI-002524 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization employs organization-defined out-of-band channels for the electronic transmission or physical delivery of organization-defined information, information system components, or devices to organization-defined individuals or information systems.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-37

---

**CCI:** CCI-002525 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization defines the security safeguards to be employed to ensure only organization-defined individuals or information systems receive organization-defined information, information system components, or devices.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-37 (1)

---

**CCI:** CCI-002526 **Status:** draft

**Contributor:** DISA FSO **Published** 2013-07-02

**Date:**

**Definition:** The organization defines the information, information system components, or devices which are to be received only by organization-defined individuals or information systems.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-37 (1)

---

**CCI:** CCI-002527 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization employs organization-defined security safeguards to ensure only organization-defined individuals or information systems receive the organization-defined information, information system components, or devices.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-37 (1)

---

**CCI:** CCI-002528 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization defines the operations security safeguards to be employed to protect key organizational information throughout the system development life cycle.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-38

---

**CCI:** CCI-002529 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization employs organization-defined operations security safeguards to protect key organizational information throughout the system development life cycle.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-38

---

**CCI:** CCI-002530 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The information system maintains a separate execution domain for each executing process.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-39

---

**CCI:** CCI-002531 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The information system implements underlying hardware separation mechanisms to facilitate process separation.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-39 (1)

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002532 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |
| **Definition:** | The organization defines the multi-threaded processing in which a separate execution domain is maintained by the information system for each thread. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SC-39 (2) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002533 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |
| **Definition:** | The information system maintains a separate execution domain for each thread in organization-defined multi-threaded processing. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SC-39 (2) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002534 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |
| **Definition:** | The organization defines types of signal parameter attacks or references to sources for such attacks from which the information system protects organization-defined wireless links. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SC-40 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002535 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |
| **Definition:** | The organization defines the external and internal wireless links the information system is to protect from organization-defined types of signal parameter attacks or references to sources for such attacks. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SC-40 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002536 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |
| **Definition:** | The information system protects organization-defined external and internal wireless links from organization-defined types of signal parameter attacks or references to sources for such attacks. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SC-40 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002537 | **Status:** | draft |

| | | | |
|---|---|---|---|
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |
| **Definition:** | The organization defines the level of protection against the effects of intentional electromagnetic interference to be achieved by implemented cryptographic mechanisms. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SC-40 (1) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002538 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |
| **Definition:** | The information system implements cryptographic mechanisms that achieve an organization-defined level of protection against the effects of intentional electromagnetic interference. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SC-40 (1) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002539 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |
| **Definition:** | The organization defines the level of reduction the information system is to implement to reduce the detection potential of wireless links. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SC-40 (2) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002540 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |
| **Definition:** | The information system implements cryptographic mechanisms to reduce the detection potential of wireless links to an organization-defined level of reduction. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SC-40 (2) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002541 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |
| **Definition:** | The information system implements cryptographic mechanisms to identify and reject wireless transmissions that are deliberate attempts to achieve imitative or manipulative communications deception based on signal parameters. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SC-40 (3) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002542 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |
| **Definition:** | The organization defines the wireless transmitters that are to have cryptographic | | |

mechanisms implemented by the information system to prevent the identification of the wireless transmitters.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-40 (4)

---

**CCI:** CCI-002543 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The information system implements cryptographic mechanisms to prevent the identification of organization-defined wireless transmitters by using the transmitter signal parameters.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-40 (4)

---

**CCI:** CCI-002544 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization defines the information systems or information system components on which organization-defined connection ports or input/output devices are to be physically disabled or removed.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-41

---

**CCI:** CCI-002545 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization defines the connection ports or input/output devices that are to be physically disabled or removed from organization-defined information systems or information system components.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-41

---

**CCI:** CCI-002546 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization physically disables or removes organization-defined connection ports or input/output devices on organization-defined information systems or information system components.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-41

---

**CCI:** CCI-002547 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization defines the exceptions where remote activation of sensors is allowed.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-42 a

---

**CCI:** CCI-002548 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-07-02
**Definition:** The information system prohibits the remote activation of environmental sensing capabilities except for the organization-defined exceptions where remote activation of sensors is allowed.
**Type:** technical
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-42 a

---

**CCI:** CCI-002549 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-07-02
**Definition:** The organization defines the class of users to receive explicit indication of sensor use.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-42 b

---

**CCI:** CCI-002550 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-07-02
**Definition:** The information system provides an explicit indication of sensor use to the organization-defined class of users.
**Type:** technical
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-42 b

---

**CCI:** CCI-002551 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-07-02
**Definition:** The organization defines the sensors to be configured so that collected data or information is reported only to authorized individuals or roles.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-42 (1)

---

**CCI:** CCI-002552 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-07-02
**Definition:** The organization ensures that the information system is configured so that data or information collected by the organization-defined sensors is only reported to authorized individuals or roles.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-42 (1)

---

**CCI:** CCI-002553 **Status:** draft
**Contributor:** DISA FSO **Published** 2013-07-02

**Date:**

**Definition:** The organization defines the measures to be employed to ensure data or information collected by organization-defined sensors is used only for authorized purposes.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-42 (2)

---

**CCI:** CCI-002554 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization defines the sensors that are to collect data or information for authorized purposes.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-42 (2)

---

**CCI:** CCI-002555 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization employs organization-defined measures, so that data or information collected by organization-defined sensors is only used for authorized purposes.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-42 (2)

---

**CCI:** CCI-002556 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization defines the environmental sensing capabilities prohibited on devices used in organization-defined facilities, areas, or systems.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-42 (3)

---

**CCI:** CCI-002557 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization defines the facilities, areas, or systems where devices processing organization-defined environmental sensing capabilities are prohibited.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-42 (3)

---

**CCI:** CCI-002558 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-02

**Definition:** The organization prohibits the use of devices possessing organization-defined environmental sensing capabilities in organization-defined facilities, areas, or systems.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-42 (3)

**CCI:** CCI-002559 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-07-02
**Definition:** The organization defines the information system components for which usage restrictions and implementation guidance are to be established.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-43 a

---

**CCI:** CCI-002560 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-07-02
**Definition:** The organization establishes usage restrictions and implementation guidance for organization-defined information system components based on the potential to cause damage to the information system if used maliciously.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-43 a

---

**CCI:** CCI-002561 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-07-02
**Definition:** The organization authorizes the use of organization-defined information system components which have the potential to cause damage to the information system if used maliciously.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-43 b

---

**CCI:** CCI-002562 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-07-02
**Definition:** The organization monitors the use of organization-defined information system components which have the potential to cause damage to the information system if used maliciously.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-43 b

---

**CCI:** CCI-002563 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-07-02
**Definition:** The organization controls the use of organization-defined information system components which have the potential to cause damage to the information system if used maliciously.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-43 b

---

**CCI:** CCI-002564 **Status:** draft
**Contributor:** DISA FSO **Published** 2013-07-02

| | | | |
|---|---|---|---|
| | | **Date:** | |

**Definition:** The organization defines the information system, system component, or location where a detonation chamber (i.e., dynamic execution environments) capability is employed.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-44

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002565 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |

**Definition:** The organization employs a detonation chamber (i.e., dynamic execution environments) capability within an organization-defined information system, system component, or location.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-44

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002523 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-02 |

**Definition:** The organization defines the individuals or information systems authorized to be recipients of organization-defined information, information system components, or devices to be delivered by employing organization-defined out-of-band channels for electronic transmission or physical delivery.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SC-37, SC-37 (1)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003544 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-08 |

**Definition:** The organization defines the frequency on which it will update the inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing personally identifiable information (PII).

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SE-1 a

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003545 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-08 |

**Definition:** The organization establishes an inventory that contains a listing of all programs identified as collecting, using, maintaining, or sharing personally identifiable information (PII).

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SE-1 a

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003546 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-08 |

**Definition:** The organization establishes an inventory that contains a listing of all information systems identified as collecting, using, maintaining, or sharing personally identifiable information (PII).

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SE-1 a

---

**CCI:** CCI-003547 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-08

**Definition:** The organization maintains an inventory that contains a listing of all programs identified as collecting, using, maintaining, or sharing personally identifiable information (PII).

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SE-1 a

---

**CCI:** CCI-003548 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-08

**Definition:** The organization maintains an inventory that contains a listing of all information systems identified as collecting, using, maintaining, or sharing personally identifiable information (PII).

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SE-1 a

---

**CCI:** CCI-003549 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-08

**Definition:** The organization updates, per organization-defined frequency, an inventory that contains a listing of all programs identified as collecting, using, maintaining, or sharing personally identifiable information (PII).

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SE-1 a

---

**CCI:** CCI-003550 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-08

**Definition:** The organization updates, per organization-defined frequency, an inventory that contains a listing of all information systems identified as collecting, using, maintaining, or sharing personally identifiable information (PII).

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SE-1 a

---

**CCI:** CCI-003551 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-08

**Definition:** The organization defines the frequency for providing each update of the personally identifiable information (PII) inventory to the CIO or information security official.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SE-1 b

---

**CCI:** CCI-003552 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-08

**Definition:** The organization provides each update of the personally identifiable information (PII) inventory to the CIO or information security official, per organization-defined frequency, to support the establishment of information security requirements for all new or modified information systems containing PII.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SE-1 b

---

**CCI:** CCI-003553 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-08

**Definition:** The organization develops a Privacy Incident Response Plan.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SE-2 a

---

**CCI:** CCI-003554 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-08

**Definition:** The organization implements a Privacy Incident Response Plan.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SE-2 a

---

**CCI:** CCI-003555 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-08

**Definition:** The organization provides an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SE-2 b

---

**CCI:** CCI-001217 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization develops and documents a system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SI-1 a
NIST: NIST SP 800-53 Revision 4 (v4): SI-1 a 1

NIST: NIST SP 800-53A (v1): SI-1.1 (i) (ii)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001218 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization disseminates the system and information integrity policy to organization-defined personnel or roles. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SI-1 a<br>NIST: NIST SP 800-53 Revision 4 (v4): SI-1 a 1<br>NIST: NIST SP 800-53A (v1): SI-1.1 (iii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001220 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization develops and documents procedures to facilitate the implementation of the system and information integrity policy and associated system integrity controls. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SI-1 b<br>NIST: NIST SP 800-53 Revision 4 (v4): SI-1 a 2<br>NIST: NIST SP 800-53A (v1): SI-1.1 (iv) (v) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001221 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization disseminates to organization-defined personnel or roles procedures to facilitate the implementation of the system and information integrity policy and associated system integrity controls. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SI-1 b<br>NIST: NIST SP 800-53 Revision 4 (v4): SI-1 a 2<br>NIST: NIST SP 800-53A (v1): SI-1.1 (vi) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002601 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The organization defines the personnel or roles to whom the system and information integrity policy and procedures are to be disseminated. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-1 a | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001219 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |

**Definition:** The organization reviews and updates system and information integrity policy in accordance with organization-defined frequency.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SI-1 a
NIST: NIST SP 800-53 Revision 4 (v4): SI-1 b 1
NIST: NIST SP 800-53A (v1): SI-1.2 (ii)

---

**CCI:** CCI-001222 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization reviews and updates system and information integrity procedures in accordance with organization-defined frequency.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SI-1 b
NIST: NIST SP 800-53 Revision 4 (v4): SI-1 b 2
NIST: NIST SP 800-53A (v1): SI-1.2 (iv)

---

**CCI:** CCI-001223 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization defines the frequency of system and information integrity policy reviews and updates.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SI-1 a
NIST: NIST SP 800-53 Revision 4 (v4): SI-1 b 1
NIST: NIST SP 800-53A (v1): SI-1.2 (i)

---

**CCI:** CCI-001224 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization defines the frequency of system and information integrity procedure reviews and updates.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SI-1 b
NIST: NIST SP 800-53 Revision 4 (v4): SI-1 b 2
NIST: NIST SP 800-53A (v1): SI-1.2 (iii)

---

**CCI:** CCI-001225 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization identifies information system flaws.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SI-2 a
NIST: NIST SP 800-53 Revision 4 (v4): SI-2 a

NIST: NIST SP 800-53A (v1): SI-2.1 (i)

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001226 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization reports information system flaws. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SI-2 a<br>NIST: NIST SP 800-53 Revision 4 (v4): SI-2 a<br>NIST: NIST SP 800-53A (v1): SI-2.1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001227 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization corrects information system flaws. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SI-2 a<br>NIST: NIST SP 800-53 Revision 4 (v4): SI-2 a<br>NIST: NIST SP 800-53A (v1): SI-2.1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001228 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization tests software updates related to flaw remediation for effectiveness before installation. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SI-2 b<br>NIST: NIST SP 800-53 Revision 4 (v4): SI-2 b<br>NIST: NIST SP 800-53A (v1): SI-2.1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001229 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization tests software updates related to flaw remediation for potential side effects before installation. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SI-2 b<br>NIST: NIST SP 800-53 Revision 4 (v4): SI-2 b<br>NIST: NIST SP 800-53A (v1): SI-2.1 (iii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002602 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The organization tests firmware updates related to flaw remediation for effectiveness before | | |

installation.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-2 b

---

**CCI:** CCI-002603 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization tests firmware updates related to flaw remediation for potential side effects before installation.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-2 b

---

**CCI:** CCI-002604 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization defines the time period following the release of updates within which security-related software updates are to be installed.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-2 c

---

**CCI:** CCI-002605 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization installs security-relevant software updates within an organization-defined time period of the release of the updates.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-2 c

---

**CCI:** CCI-002606 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization defines the time period following the release of updates within which security-related firmware updates are to be installed.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-2 c

---

**CCI:** CCI-002607 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization installs security-relevant firmware updates within an organization-defined time period of the release of the updates.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-2 c

---

**CCI:** CCI-001230 **Status:** draft

| | | | |
|---|---|---|---|
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization incorporates flaw remediation into the organizational configuration management process. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SI-2 c<br>NIST: NIST SP 800-53 Revision 4 (v4): SI-2 d<br>NIST: NIST SP 800-53A (v1): SI-2.1 (iv) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001231 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization centrally manages the flaw remediation process. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SI-2 (1)<br>NIST: NIST SP 800-53 Revision 4 (v4): SI-2 (1)<br>NIST: NIST SP 800-53A (v1): SI-2 (1).1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001233 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization employs automated mechanisms on an organization-defined frequency to determine the state of information system components with regard to flaw remediation. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): SI-2 (2)<br>NIST: NIST SP 800-53 Revision 4 (v4): SI-2 (2)<br>NIST: NIST SP 800-53A (v1): SI-2 (2).1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001234 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization defines a frequency for employing automated mechanisms to determine the state of information system components with regard to flaw remediation. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SI-2 (2)<br>NIST: NIST SP 800-53 Revision 4 (v4): SI-2 (2)<br>NIST: NIST SP 800-53A (v1): SI-2 (2).1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001235 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization measures the time between flaw identification and flaw remediation. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SI-2 (3) | | |

NIST: NIST SP 800-53 Revision 4 (v4): SI-2 (3) (a)
NIST: NIST SP 800-53A (v1): SI-2 (3).1 (ii)

---

**CCI:** CCI-001236 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-22
**Definition:** The organization defines benchmarks for the time taken to apply corrective actions after flaw identification.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): SI-2 (3)
NIST: NIST SP 800-53 Revision 4 (v4): SI-2 (3) (b)
NIST: NIST SP 800-53A (v1): SI-2 (3).1 (i)

---

**CCI:** CCI-002608 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-07-11
**Definition:** The organization establishes organization-defined benchmarks for the time taken to apply corrective actions after flaw identification.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-2 (3) (b)

---

**CCI:** CCI-002609 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-07-11
**Definition:** The organization defines the information system components on which organization-defined security-relevant software updates will be automatically installed.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-2 (5)

---

**CCI:** CCI-002610 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-07-11
**Definition:** The organization defines the information system components on which organization-defined security-relevant firmware updates will be automatically installed.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-2 (5)

---

**CCI:** CCI-002611 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-07-11
**Definition:** The organization defines the security-relevant software updates to be automatically installed on organization-defined information system components.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-2 (5)

---

**CCI:** CCI-002612
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2013-07-11
**Definition:** The organization defines the security-relevant firmware updates to be automatically installed on organization-defined information system components.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-2 (5)

---

**CCI:** CCI-002613
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2013-07-11
**Definition:** The organization installs organization-defined security-relevant software updates automatically to organization-defined information system components.
**Type:** technical
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-2 (5)

---

**CCI:** CCI-002614
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2013-07-11
**Definition:** The organization installs organization-defined security-relevant firmware updates automatically to organization-defined information system components.
**Type:** technical
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-2 (5)

---

**CCI:** CCI-002615
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2013-07-11
**Definition:** The organization defines the software components to be removed (e.g., previous versions) after updated versions have been installed.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-2 (6)

---

**CCI:** CCI-002616
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2013-07-11
**Definition:** The organization defines the firmware components to be removed (e.g., previous versions) after updated versions have been installed.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-2 (6)

---

**CCI:** CCI-002617
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2013-07-11
**Definition:** The organization removes organization-defined software components (e.g., previous versions) after updated versions have been installed.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-2 (6)

---

**CCI:** CCI-002618 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization removes organization-defined firmware components (e.g., previous versions) after updated versions have been installed.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-2 (6)

---

**CCI:** CCI-002619 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization employs malicious code protection mechanisms at information system entry points to detect malicious code.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-3 a

---

**CCI:** CCI-002620 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization employs malicious code protection mechanisms at information system exit points to detect malicious code.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-3 a

---

**CCI:** CCI-002621 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization employs malicious code protection mechanisms at information system entry points to eradicate malicious code.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-3 a

---

**CCI:** CCI-002622 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization employs malicious code protection mechanisms at information system exit points to eradicate malicious code.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-3 a

---

**CCI:** CCI-001240 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SI-3 b
NIST: NIST SP 800-53 Revision 4 (v4): SI-3 b
NIST: NIST SP 800-53A (v1): SI-3.1 (iii)

---

**CCI:** CCI-001241 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization configures malicious code protection mechanisms to perform periodic scans of the information system on an organization-defined frequency.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SI-3 c
NIST: NIST SP 800-53 Revision 4 (v4): SI-3 c 1
NIST: NIST SP 800-53A (v1): SI-3.1 (vi)

---

**CCI:** CCI-001242 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization configures malicious code protection mechanisms to perform real-time scans of files from external sources at endpoints as the files are downloaded, opened, or executed in accordance with organizational security policy.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SI-3 c
NIST: NIST SP 800-53 Revision 4 (v4): SI-3 c 1
NIST: NIST SP 800-53A (v1): SI-3.1 (vi)

---

**CCI:** CCI-001243 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization configures malicious code protection mechanisms to perform organization-defined action(s) in response to malicious code detection.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SI-3 c
NIST: NIST SP 800-53 Revision 4 (v4): SI-3 c 2
NIST: NIST SP 800-53A (v1): SI-3.1 (vi)

---

**CCI:** CCI-001244 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization defines one or more actions to perform in response to malicious code detection, such as blocking malicious code, quarantining malicious code, or sending alerts to administrators.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SI-3 c
NIST: NIST SP 800-53 Revision 4 (v4): SI-3 c 2
NIST: NIST SP 800-53A (v1): SI-3.1 (v)

---

**CCI:** CCI-002623
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2013-07-11

**Definition:** The organization defines the frequency for performing periodic scans of the information system for malicious code.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-3 c 1

---

**CCI:** CCI-002624
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2013-07-11

**Definition:** The organization configures malicious code protection mechanisms to perform real-time scans of files from external sources at network entry/exit points as the files are downloaded, opened, or executed in accordance with organizational security policy.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-3 c 1

---

**CCI:** CCI-001245
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2009-09-22

**Definition:** The organization addresses the receipt of false positives during malicious code detection and eradication, and the resulting potential impact on the availability of the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SI-3 d
NIST: NIST SP 800-53 Revision 4 (v4): SI-3 d
NIST: NIST SP 800-53A (v1): SI-3.1 (vii)

---

**CCI:** CCI-001246
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2009-09-22

**Definition:** The organization centrally manages malicious code protection mechanisms.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SI-3 (1)
NIST: NIST SP 800-53 Revision 4 (v4): SI-3 (1)
NIST: NIST SP 800-53A (v1): SI-3 (1).1

---

**CCI:** CCI-001247 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The information system automatically updates malicious code protection mechanisms.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SI-3 (2)
NIST: NIST SP 800-53 Revision 4 (v4): SI-3 (2)
NIST: NIST SP 800-53A (v1): SI-3 (2).1

---

**CCI:** CCI-001249 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The information system updates malicious code protection mechanisms only when directed by a privileged user.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SI-3 (4)
NIST: NIST SP 800-53 Revision 4 (v4): SI-3 (4)
NIST: NIST SP 800-53A (v1): SI-3 (4).1

---

**CCI:** CCI-001669 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2010-05-12

**Definition:** The organization defines the frequency of testing malicious code protection mechanisms.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SI-3 (6)
NIST: NIST SP 800-53 Revision 4 (v4): SI-3 (6) (a)
NIST: NIST SP 800-53A (v1): SI-3 (6).1 (i)

---

**CCI:** CCI-001251 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization tests malicious code protection mechanisms on an organization-defined frequency by introducing a known benign, non-spreading test case into the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SI-3 (6)
NIST: NIST SP 800-53 Revision 4 (v4): SI-3 (6) (a)
NIST: NIST SP 800-53A (v1): SI-3 (6).1 (ii)

---

**CCI:** CCI-002625 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization, when testing malicious code protection mechanisms, verifies the detection of the test case occurs.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-3 (6) (b)

---

**CCI:** CCI-002626 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization, when testing malicious code protection mechanisms, verifies the incident reporting of the test case occurs.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-3 (6) (b)

---

**CCI:** CCI-002627 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The information system implements nonsignature-based malicious code detection mechanisms.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-3 (7)

---

**CCI:** CCI-002628 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization defines the unauthorized operating system commands that are to be detected through the kernel application programming interface by organization-defined information system hardware components.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-3 (8)

---

**CCI:** CCI-002629 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization defines the information system hardware components that are to detect organization-defined unauthorized operating system commands through the kernel programming application interface.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-3 (8)

---

**CCI:** CCI-002630 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The information system detects organization-defined unauthorized operating system commands through the kernel application programming interface at organization-defined information system hardware components.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-3 (8)

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002631 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |

**Definition:** The information system issues a warning, audits the command execution, or prevents the execution of the command when organization-defined unauthorized operating system commands are detected.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-3 (8)

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002632 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |

**Definition:** The organization defines the remote commands that are to be authenticated using organization-defined safeguards for malicious code protection.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-3 (9)

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002633 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |

**Definition:** The organization defines the security safeguards to be implemented to authenticate organization-defined remote commands for malicious code protection.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-3 (9)

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002637 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |

**Definition:** The information system implements organization-defined security safeguards to authenticate organization-defined remote commands for malicious code protection.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-3 (9)

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002634 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |

**Definition:** The organization defines the tools to be employed to analyze the characteristics and behavior of malicious code.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-3 (10) (a)

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002635 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |

| | | | |
|---|---|---|---|
| **Definition:** | The organization defines the techniques to be employed to analyze the characteristics and behavior of malicious code. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-3 (10) (a) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002636 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The organization employs organization-defined tools to analyze the characteristics and behavior of malicious code. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-3 (10) (a) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002638 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The organization employs organization-defined techniques to analyze the characteristics and behavior of malicious code. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-3 (10) (a) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002639 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The organization incorporates the results from malicious code analysis into organizational incident response processes. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-3 (10) (b) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002640 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The organization incorporates the results from malicious code analysis into organizational flaw remediation processes. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-3 (10) (b) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002653 | **Status:** | deprecated |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The organization provides organization-defined information system monitoring information to organization-defined personnel or roles as needed or per organization-defined frequency. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-4 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001253 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization defines the objectives of monitoring for attacks and indicators of potential attacks on the information system. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SI-4 a<br>NIST: NIST SP 800-53 Revision 4 (v4): SI-4 a 1<br>NIST: NIST SP 800-53A (v1): SI-4.1 (i) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002641 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The organization monitors the information system to detect attacks and indicators of potential attacks in accordance with organization-defined monitoring objectives. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-4 a 1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002642 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The organization monitors the information system to detect unauthorized local connections. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-4 a 2 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002643 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The organization monitors the information system to detect unauthorized network connections. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-4 a 2 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002644 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The organization monitors the information system to detect unauthorized remote connections. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-4 a 2 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002645 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |

**Definition:** The organization defines the techniques and methods to be used to identify unauthorized use of the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-4 b

---

**CCI:** CCI-002646 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization identifies unauthorized use of the information system through organization-defined techniques and methods.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-4 b

---

**CCI:** CCI-001255 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization deploys monitoring devices strategically within the information system to collect organization-determined essential information.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SI-4 c
NIST: NIST SP 800-53 Revision 4 (v4): SI-4 c
NIST: NIST SP 800-53A (v1): SI-4.1 (iv)

---

**CCI:** CCI-001256 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization deploys monitoring devices at ad hoc locations within the system to track specific types of transactions of interest to the organization.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SI-4 c
NIST: NIST SP 800-53 Revision 4 (v4): SI-4 c
NIST: NIST SP 800-53A (v1): SI-4.1 (iv)

---

**CCI:** CCI-002647 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization protects information obtained from intrusion-monitoring tools from unauthorized access.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-4 d

---

**CCI:** CCI-002648 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization protects information obtained from intrusion-monitoring tools from unauthorized modification.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-4 d

---

**CCI:** CCI-002649 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization protects information obtained from intrusion-monitoring tools from unauthorized deletion.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-4 d

---

**CCI:** CCI-001257 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SI-4 d

NIST: NIST SP 800-53 Revision 4 (v4): SI-4 e

NIST: NIST SP 800-53A (v1): SI-4.1 (v)

---

**CCI:** CCI-001258 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SI-4 e

NIST: NIST SP 800-53 Revision 4 (v4): SI-4 f

NIST: NIST SP 800-53A (v1): SI-4.1 (vi)

---

**CCI:** CCI-002650 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization defines the information system monitoring information that is to be provided the organization-defined personnel or roles.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-4 g

---

**CCI:** CCI-002651 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization defines the personnel or roles that are to be provided organization-defined information system monitoring information.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-4 g

---

**CCI:** CCI-002652 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization defines the frequency at which the organization will provide the organization-defined information system monitoring information to organization-defined personnel or roles.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-4 g

---

**CCI:** CCI-002654 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization provides organization-defined information system monitoring information to organization-defined personnel or roles as needed or per organization-defined frequency.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-4 g

---

**CCI:** CCI-002655 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization connects individual intrusion detection tools into an information system-wide intrusion detection system.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (1)

---

**CCI:** CCI-002656 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization configures individual intrusion detection tools into an information system-wide intrusion detection system.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (1)

---

**CCI:** CCI-001260 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization employs automated tools to support near real-time analysis of events.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SI-4 (2)
NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (2)
NIST: NIST SP 800-53A (v1): SI-4 (2).1

---

**CCI:** CCI-002657 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-07-11
**Definition:** The organization employs automated tools to integrate intrusion detection tools into access control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (3)

---

**CCI:** CCI-002658 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-07-11
**Definition:** The organization employs automated tools to integrate intrusion detection tools into flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (3)

---

**CCI:** CCI-002659 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-07-11
**Definition:** The organization defines the frequency on which it will monitor inbound communications for unusual or unauthorized activities or conditions.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (4)

---

**CCI:** CCI-002660 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-07-11
**Definition:** The organization defines the frequency on which it will monitor outbound communications for unusual or unauthorized activities or conditions.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (4)

---

**CCI:** CCI-002661 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-07-11
**Definition:** The information system monitors inbound communications traffic per organization-defined frequency for unusual or unauthorized activities or conditions.
**Type:** technical
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (4)

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002662 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The information system monitors outbound communications traffic per organization-defined frequency for unusual or unauthorized activities or conditions. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (4) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001264 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization defines indicators of compromise or potential compromise to the security of the information system which will result in information system alerts being provided to organization-defined personnel or roles. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SI-4 (5)<br>NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (5)<br>NIST: NIST SP 800-53A (v1): SI-4 (5).1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002663 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The organization defines the personnel or roles to receive information system alerts when organization-defined indicators of compromise or potential compromise occur. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (5) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002664 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The information system alerts organization-defined personnel or roles when organization-defined compromise indicators reflect the occurrence of a compromise or a potential compromise. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (5) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001670 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-12 |
| **Definition:** | The information system takes organization-defined least-disruptive actions to terminate suspicious events. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): SI-4 (7)<br>NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (7) | | |

|  |  |  |  |
|---|---|---|---|
|  | NIST: NIST SP 800-53A (v1): SI-4 (7).1 (iv) |  |  |

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-001266 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The information system notifies an organization-defined list of incident response personnel (identified by name and/or by role) of detected suspicious events. |  |  |
| **Type:** | technical |  |  |
| **References:** | NIST: NIST SP 800-53 (v3): SI-4 (7)<br>NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (7)<br>NIST: NIST SP 800-53A (v1): SI-4 (7).1 (iii) |  |  |

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-001267 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization defines a list of incident response personnel (identified by name and/or by role) to be notified of detected suspicious events. |  |  |
| **Type:** | policy |  |  |
| **References:** | NIST: NIST SP 800-53 (v3): SI-4 (7)<br>NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (7)<br>NIST: NIST SP 800-53A (v1): SI-4 (7).1 (i) |  |  |

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-001268 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization defines a list of least-disruptive actions to be taken by the information system to terminate suspicious events. |  |  |
| **Type:** | policy |  |  |
| **References:** | NIST: NIST SP 800-53 (v3): SI-4 (7)<br>NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (7)<br>NIST: NIST SP 800-53A (v1): SI-4 (7).1 (ii) |  |  |

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-001270 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization tests intrusion monitoring tools at an organization-defined frequency. |  |  |
| **Type:** | policy |  |  |
| **References:** | NIST: NIST SP 800-53 (v3): SI-4 (9)<br>NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (9)<br>NIST: NIST SP 800-53A (v1): SI-4 (9).1 (ii) |  |  |

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-001271 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |

**Definition:** The organization defines the frequency for testing intrusion monitoring tools.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SI-4 (9)
NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (9)
NIST: NIST SP 800-53A (v1): SI-4 (9).1 (i)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002665 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |

**Definition:** The organization defines the encrypted communications traffic that is to be visible to organization-defined information system monitoring tools.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (10)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002666 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |

**Definition:** The organization defines the information system monitoring tools that will have visibility into organization-defined encrypted communications traffic.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (10)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002667 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |

**Definition:** The organization makes provisions so that organization-defined encrypted communications traffic is visible to organization-defined information system monitoring tools.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (10)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001671 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-12 |

**Definition:** The organization analyzes outbound communications traffic at selected organization-defined interior points within the system (e.g., subnetworks, subsystems) to discover anomalies.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SI-4 (11)
NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (11)
NIST: NIST SP 800-53A (v1): SI-4 ( 11).1

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001273 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |

**Definition:** The organization analyzes outbound communications traffic at the external boundary of the information system to discover anomalies.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SI-4 (11)
NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (11)
NIST: NIST SP 800-53A (v1): SI-4 (11).1

---

**CCI:** CCI-002668 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization defines the interior points within the information system (e.g., subnetworks, subsystems) where outbound communications will be analyzed to discover anomalies.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (11)

---

**CCI:** CCI-001274 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization employs automated mechanisms to alert security personnel of organization-defined inappropriate or unusual activities with security implications.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SI-4 (12)
NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (12)
NIST: NIST SP 800-53A (v1): SI-4 (12).1 (ii)

---

**CCI:** CCI-001275 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization defines the activities which will trigger alerts to security personnel of inappropriate or unusual activities.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SI-4 (12)
NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (12)
NIST: NIST SP 800-53A (v1): SI-4 (12).1 (i)

---

**CCI:** CCI-001276 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization analyzes communications traffic/event patterns for the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SI-4 (13) (a)
NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (13) (a)
NIST: NIST SP 800-53A (v1): SI-4 (13).1 (i)

---

**CCI:** CCI-001277
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2009-09-22
**Definition:** The organization develops profiles representing common traffic patterns and/or events.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): SI-4 (13) (b)
NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (13) (b)
NIST: NIST SP 800-53A (v1): SI-4 (13).1 (ii)

---

**CCI:** CCI-002669
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2013-07-11
**Definition:** The organization uses the traffic/event profiles in tuning system-monitoring devices to reduce the number of false positives and false negatives.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (13) (c)

---

**CCI:** CCI-001673
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2010-05-12
**Definition:** The organization employs a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): SI-4 (14)
NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (14)
NIST: NIST SP 800-53A (v1): SI-4 (14).1 (iii)

---

**CCI:** CCI-001282
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2009-09-22
**Definition:** The organization employs an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): SI-4 (15)
NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (15)
NIST: NIST SP 800-53A (v1): SI-4 (15).1

---

**CCI:** CCI-001283
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2009-09-22
**Definition:** The organization correlates information from monitoring tools employed throughout the information system.
**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SI-4 (16)
NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (16)
NIST: NIST SP 800-53A (v1): SI-4 (16).1

---

**CCI:** CCI-001284 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-22
**Definition:** The organization correlates information from monitoring physical, cyber, and supply chain activities to achieve integrated, organization-wide situational awareness.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): SI-4 (17)
NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (17)
NIST: NIST SP 800-53A (v1): SI-4 (17).1

---

**CCI:** CCI-002670 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-07-11
**Definition:** The organization defines the interior points within the system (e.g., subsystems, subnetworks) where outbound communications will be analyzed to detect covert exfiltration of information.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (18)

---

**CCI:** CCI-002671 **Status:** draft
**Contributor:** **Published Date:** 2013-07-11
**Definition:** The organization analyzes outbound communications traffic at the external boundary of the information system (i.e., system perimeter) to detect covert exfiltration of information.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (18)

---

**CCI:** CCI-002672 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-07-11
**Definition:** The organization analyzes outbound communications traffic at organization-defined interior points within the system (e.g., subsystems, subnetworks) to detect covert exfiltration of information.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (18)

---

**CCI:** CCI-002673 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-07-11
**Definition:** The organization defines the additional monitoring to be implemented for individuals identified as posing an increased level of risk.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (19)

---

**CCI:** CCI-002674 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization defines the sources that may be used to identify individuals who pose an increased level of risk.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (19)

---

**CCI:** CCI-002675 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization implements organization-defined additional monitoring of individuals who have been identified by organization-defined sources as posing an increased level of risk.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (19)

---

**CCI:** CCI-002676 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization defines additional monitoring to be implemented for privileged users.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (20)

---

**CCI:** CCI-002677 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization implements organization-defined additional monitoring of privileged users.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (20)

---

**CCI:** CCI-002678 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization defines additional monitoring to be implemented for individuals during an organization-defined probationary period.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (21)

---

**CCI:** CCI-002679 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization defines the probationary period during which additional monitoring will be implemented for individuals.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (21)

---

**CCI:** CCI-002680 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization implements organization-defined additional monitoring of individuals during an organization-defined probationary period.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (21)

---

**CCI:** CCI-002681 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization defines the authorization or approval process for network services.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (22)

---

**CCI:** CCI-002682 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization defines the personnel or roles to be alerted when unauthorized or unapproved network services are detected.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (22)

---

**CCI:** CCI-002683 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The information system detects network services that have not been authorized or approved by the organization-defined authorization or approval processes.

**Type:** policy, technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (22)

---

**CCI:** CCI-002684 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The information system audits and/or alerts organization-defined personnel when unauthorized network services are detected.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (22)

---

**CCI:** CCI-002685 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization defines the host-based monitoring mechanisms to be implemented at organization-defined information system components.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (23)

---

**CCI:** CCI-002686 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization defines the information system components at which organization-defined host-based monitoring mechanisms are to be implemented.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (23)

---

**CCI:** CCI-002687 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization implements organization-defined host-based monitoring mechanisms at organization-defined information system components.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (23)

---

**CCI:** CCI-002688 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The information system discovers indicators of compromise.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (24)

---

**CCI:** CCI-002689 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The information system collects indicators of compromise.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (24)

---

**CCI:** CCI-002690 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The information system distributes indicators of compromise.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (24)

---

**CCI:** CCI-002691 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The information system uses indicators of compromise.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-4 (24)

---

**CCI:** CCI-001285 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization receives information system security alerts, advisories, and directives from organization-defined external organizations on an ongoing basis.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SI-5 a

NIST: NIST SP 800-53 Revision 4 (v4): SI-5 a

NIST: NIST SP 800-53A (v1): SI-5.1 (i)

---

**CCI:** CCI-002692 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization defines the external organizations from which it receives information system security alerts, advisories, and directives.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-5 a

---

**CCI:** CCI-001286 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization generates internal security alerts, advisories, and directives as deemed necessary.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SI-5 b

NIST: NIST SP 800-53 Revision 4 (v4): SI-5 b

NIST: NIST SP 800-53A (v1): SI-5.1 (ii)

---

**CCI:** CCI-001287 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization disseminates security alerts, advisories, and directives to organization-defined personnel or roles, organization-defined elements within the organization, and/or organization-defined external organizations.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SI-5 c

NIST: NIST SP 800-53 Revision 4 (v4): SI-5 c

NIST: NIST SP 800-53A (v1): SI-5.1 (iv)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001288 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization defines the personnel or roles to whom the organization will disseminate security alerts, advisories, and directives. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SI-5 c<br>NIST: NIST SP 800-53 Revision 4 (v4): SI-5 c<br>NIST: NIST SP 800-53A (v1): SI-5.1 (iii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002693 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The organization defines the elements within the organization to whom the organization will disseminate security alerts, advisories, and directives. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-5 c | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002694 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The organization defines the external organizations to which the organization will disseminate security alerts, advisories, and directives. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-5 c | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001289 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SI-5 d<br>NIST: NIST SP 800-53 Revision 4 (v4): SI-5 d<br>NIST: NIST SP 800-53A (v1): SI-5.1 (v) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001290 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization employs automated mechanisms to make security alert and advisory information available throughout the organization. | | |
| **Type:** | policy | | |

**References:** NIST: NIST SP 800-53 (v3): SI-5 (1)
NIST: NIST SP 800-53 Revision 4 (v4): SI-5 (1)
NIST: NIST SP 800-53A (v1): SI-5 (1).1

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002695 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |

**Definition:** The organization defines the security functions that require verification of correct operation.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-6 a

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002696 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |

**Definition:** The information system verifies correct operation of organization-defined security functions.
**Type:** technical
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-6 a

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002697 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |

**Definition:** The organization defines the frequency at which it will verify correct operation of organization-defined security functions.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-6 b

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002698 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |

**Definition:** The organization defines the system transitional states when the information system will verify correct operation of organization-defined security functions.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-6 b

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002699 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |

**Definition:** The information system performs verification of the correct operation of organization-defined security functions: when the system is in an organization-defined transitional state; upon command by a user with appropriate privileges; and/or on an organization-defined frequency.
**Type:** technical
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-6 b

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001294 | **Status:** | draft |

| | | | |
|---|---|---|---|
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The information system notifies organization-defined personnel or roles of failed security verification tests. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): SI-6 (1)<br>NIST: NIST SP 800-53 Revision 4 (v4): SI-6 c<br>NIST: NIST SP 800-53A (v1): SI-6 (1).1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002700 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The organization defines the personnel or roles to be notified when security verification tests fail. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-6 c | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002701 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The organization defines alternative action(s) to be taken when the information system discovers anomalies in the operation of organization-defined security functions. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-6 d | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002702 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The information system shuts the information system down, restarts the information system, and/or initiates organization-defined alternative action(s) when anomalies in the operation of the organization-defined security functions are discovered. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-6 d | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001295 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The information system implements automated mechanisms to support the management of distributed security testing. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): SI-6 (2)<br>NIST: NIST SP 800-53 Revision 4 (v4): SI-6 (2)<br>NIST: NIST SP 800-53A (v1): SI-6 (2).1 | | |

---

**CCI:** CCI-001675 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2010-05-12

**Definition:** The organization defines the personnel or roles that are to receive reports on the results of security function verification.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SI-6 (3)
NIST: NIST SP 800-53 Revision 4 (v4): SI-6 (3)
NIST: NIST SP 800-53A (v1): SI-6 (3).1 (i)

---

**CCI:** CCI-001296 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization reports the results of security function verification to organization-defined personnel or roles.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SI-6 (3)
NIST: NIST SP 800-53 Revision 4 (v4): SI-6 (3)
NIST: NIST SP 800-53A (v1): SI-6 (3).1 (ii)

---

**CCI:** CCI-002703 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization defines the software, firmware, and information which will be subjected to integrity verification tools to detect unauthorized changes.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-7

---

**CCI:** CCI-002704 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization employs integrity verification tools to detect unauthorized changes to organization-defined software, firmware, and information.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-7

---

**CCI:** CCI-002705 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization defines the software on which integrity checks will be performed.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-7 (1)

---

**CCI:** CCI-002706 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization defines the firmware on which integrity checks will be performed.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-7 (1)

---

**CCI:** CCI-002707 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization defines the information on which integrity checks will be performed.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-7 (1)

---

**CCI:** CCI-002708 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization defines the transitional state or security-relevant events when the information system will perform integrity checks on software, firmware, and information.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-7 (1)

---

**CCI:** CCI-002709 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization defines the frequency at which it will perform integrity checks of software, firmware, and information.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-7 (1)

---

**CCI:** CCI-002710 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The information system performs an integrity check of organization-defined software at startup, at organization-defined transitional states or security-relevant events, or on an organization-defined frequency.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-7 (1)

---

**CCI:** CCI-002711 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The information system performs an integrity check of organization-defined firmware at startup, at organization-defined transitional states or security-relevant events, or on an organization-defined frequency.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-7 (1)

---

**CCI:** CCI-002712 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The information system performs an integrity check of organization-defined information at startup, at organization-defined transitional states or security-relevant events, or on an organization-defined frequency.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-7 (1)

---

**CCI:** CCI-001300 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization employs automated tools that provide notification to organization-defined personnel or roles upon discovering discrepancies during integrity verification.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SI-7 (2)
NIST: NIST SP 800-53 Revision 4 (v4): SI-7 (2)
NIST: NIST SP 800-53A (v1): SI-7 (2).1

---

**CCI:** CCI-002713 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization defines the personnel or roles to be notified when discrepancies are discovered during integrity verification.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-7 (2)

---

**CCI:** CCI-001301 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization employs centrally managed integrity verification tools.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SI-7 (3)
NIST: NIST SP 800-53 Revision 4 (v4): SI-7 (3)
NIST: NIST SP 800-53A (v1): SI-7 (3).1

---

**CCI:** CCI-002714 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization defines the security safeguards that are to be employed when integrity violations are discovered.

**Type:** policy

| | | | |
|---|---|---|---|
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-7 (5) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002715 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The information system automatically shuts the information system down, restarts the information system, and/or implements organization-defined security safeguards when integrity violations are discovered. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-7 (5) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002716 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The information system implements cryptographic mechanisms to detect unauthorized changes to software. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-7 (6) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002717 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The information system implements cryptographic mechanisms to detect unauthorized changes to firmware. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-7 (6) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002718 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The information system implements cryptographic mechanisms to detect unauthorized changes to information. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-7 (6) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002719 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The organization defines the unauthorized security-relevant changes to the information system that are to be incorporated into the organizational incident response capability. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-7 (7) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002720 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published** | 2013-07-11 |

| | | | |
|---|---|---|---|
| | | **Date:** | |

**Definition:** The organization incorporates the detection of unauthorized organization-defined security-relevant changes to the information system into the organizational incident response capability.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-7 (7)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002721 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |

**Definition:** The organization defines the personnel or roles that are to be alerted by the information system when it detects a potential integrity violation.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-7 (8)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002722 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |

**Definition:** The organization defines other actions that can be taken when the information system detects a potential integrity violation.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-7 (8)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002723 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |

**Definition:** The information system, upon detection of a potential integrity violation, provides the capability to audit the event.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-7 (8)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002724 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |

**Definition:** The information system, upon detection of a potential integrity violation, initiates one or more of the following actions: generates an audit record; alerts the current user; alerts organization-defined personnel or roles; and/or organization-defined other actions.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-7 (8)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002725 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |

**Definition:** The organization defines the devices which will have the integrity of the boot process verified.

| | | | |
|---|---|---|---|
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-7 (9) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002726 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The information system verifies the integrity of the boot process of organization-defined devices. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-7 (9) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002727 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The organization defines the security safeguards to be implemented to protect the integrity of the boot firmware in organization-defined devices. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-7 (10) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002728 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The organization defines the devices on which organization-defined security safeguards will be implemented to protect the integrity of the boot firmware. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-7 (10) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002729 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The information system implements organization-defined security safeguards to protect the integrity of boot firmware in organization-defined devices. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-7 (10) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002730 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The organization defines the user-installed software that is to be executed in a confined physical or virtual machine environment with limited privileges. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-7 (11) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002731 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published** | 2013-07-11 |

| | | | |
|---|---|---|---|
| | | **Date:** | |
| **Definition:** | The organization requires that organization-defined user-installed software execute in a confined physical or virtual machine environment with limited privileges. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-7 (11) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002732 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The organization defines the user-installed software that is to have its integrity verified prior to execution. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-7 (12) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002733 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The organization requires that the integrity of organization-defined user-installed software be verified prior to execution. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-7 (12) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002734 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The organization defines the personnel or roles which have the authority to explicitly approve binary or machine-executable code. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-7 (13) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002735 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The organization allows execution of binary or machine-executable code obtained from sources with limited or no warranty and without the provision of source code only in confined physical or virtual machine environments. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-7 (13) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002736 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The organization allows execution of binary or machine-executable code obtained from sources with limited or no warranty and without the provision of source code only with the explicit approval of organization-defined personnel or roles. | | |

| | | | |
|---|---|---|---|
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-7 (13) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002737 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The organization prohibits the use of binary or machine-executable code from sources with limited or no warranty and without the provision of source code. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-7 (14) (a) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002738 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The organization provides exceptions to the source code requirement only for compelling mission/operational requirements and with the approval of the authorizing official. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-7 (14) (b) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002739 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The organization defines the software or firmware components on which cryptographic mechanisms are to be implemented to support authentication prior to installation. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-7 (15) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002740 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The information system implements cryptographic mechanisms to authenticate organization-defined software or firmware components prior to installation. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-7 (15) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001321 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization does not allow a process to execute without supervision for more than an organization-defined time period. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SI-13 (2)<br>NIST: NIST SP 800-53 Revision 4 (v4): SI-7 (16)<br>NIST: NIST SP 800-53A (v1): SI-13 (2).1 (ii) | | |

**CCI:** CCI-001322 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-22
**Definition:** The organization defines a time period that is the longest a process is allowed to execute without supervision.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): SI-13 (2)
NIST: NIST SP 800-53 Revision 4 (v4): SI-7 (16)
NIST: NIST SP 800-53A (v1): SI-13 (2).1 (i)

---

**CCI:** CCI-002741 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-07-11
**Definition:** The organization employs spam protection mechanisms at information system entry points to detect and take action on unsolicited messages.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-8 a

---

**CCI:** CCI-002742 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-07-11
**Definition:** The organization employs spam protection mechanisms at information system exit points to detect and take action on unsolicited messages.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-8 a

---

**CCI:** CCI-001306 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-22
**Definition:** The organization updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): SI-8 b
NIST: NIST SP 800-53 Revision 4 (v4): SI-8 b
NIST: NIST SP 800-53A (v1): SI-8.1 (iii)

---

**CCI:** CCI-001307 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-22
**Definition:** The organization centrally manages spam protection mechanisms.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): SI-8 (1)
NIST: NIST SP 800-53 Revision 4 (v4): SI-8 (1)
NIST: NIST SP 800-53A (v1): SI-8 (1).1

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001308 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The information system automatically updates spam protection mechanisms. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): SI-8 (2)<br>NIST: NIST SP 800-53 Revision 4 (v4): SI-8 (2)<br>NIST: NIST SP 800-53A (v1): SI-8 (2).1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002743 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The information system implements spam protection mechanisms with a learning capability to more effectively identify legitimate communications traffic. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-8 (3) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001310 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The information system checks the validity of organization-defined inputs. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): SI-10<br>NIST: NIST SP 800-53 Revision 4 (v4): SI-10<br>NIST: NIST SP 800-53A (v1): SI-10.1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002744 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The organization defines the inputs on which the information system is to conduct validity checks. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-10 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002745 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The organization defines the inputs for which the information system provides a manual override capability for input validation. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-10 (1) (a) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002746 | **Status:** | draft |

| | | | |
|---|---|---|---|
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The information system provides a manual override capability for input validation of organization-defined inputs. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-10 (1) (a) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002747 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The organization defines the individuals who have the authorization to use the manual override capability for input validation. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-10 (1) (b) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002748 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The information system restricts the use of the manual override capability to only organization-defined authorized individuals. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-10 (1) (b) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002749 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The information system audits the use of the manual override capability. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-10 (1) (c) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002750 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The organization defines the time period within which input validation errors are to be reviewed. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-10 (2) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002751 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The organization defines the time period within which input validation errors are to be resolved. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-10 (2) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002752 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The organization ensures that input validation errors are reviewed within an organization-defined time period. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-10 (2) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002753 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The organization ensures that input validation errors are resolved within an organization-defined time period. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-10 (2) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002754 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The information system behaves in a predictable and documented manner that reflects organizational and system objectives when invalid inputs are received. | | |
| **Type:** | policy, technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-10 (3) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002755 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The organization accounts for timing interactions among information system components in determining appropriate responses for invalid inputs. | | |
| **Type:** | policy, technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-10 (4) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002756 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The organization defines the trusted sources to which the usage of information inputs will be restricted (e.g., whitelisting). | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-10 (5) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002757 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The organization defines the acceptable formats to which information inputs are restricted. | | |

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-10 (5)

---

**CCI:** CCI-002758 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization restricts the use of information inputs to organization-defined trusted sources and/or organization-defined formats.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-10 (5)

---

**CCI:** CCI-001312 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The information system generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SI-11 b
NIST: NIST SP 800-53 Revision 4 (v4): SI-11 a
NIST: NIST SP 800-53A (v1): SI-11.1 (iii)

---

**CCI:** CCI-001314 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The information system reveals error messages only to organization-defined personnel or roles.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SI-11 c
NIST: NIST SP 800-53 Revision 4 (v4): SI-11 b
NIST: NIST SP 800-53A (v1): SI-11.1 (iv)

---

**CCI:** CCI-002759 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization defines the personnel or roles to whom error messages are to be revealed.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-11 b

---

**CCI:** CCI-001678 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2010-05-12

**Definition:** The organization retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SI-12
NIST: NIST SP 800-53 Revision 4 (v4): SI-12
NIST: NIST SP 800-53A (v1): SI-12.1 (ii)

---

**CCI:** CCI-001315 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization handles information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SI-12
NIST: NIST SP 800-53 Revision 4 (v4): SI-12
NIST: NIST SP 800-53A (v1): SI-12.1 (i)

---

**CCI:** CCI-002760 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization determines mean time to failure (MTTF) for organization-defined information system components in specific environments of operation.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-13 a

---

**CCI:** CCI-002761 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization defines the system components in specific environments of operation for which the mean time to failure (MTTF) is to be determined.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-13 a

---

**CCI:** CCI-001318 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization provides substitute information system components.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SI-13 b
NIST: NIST SP 800-53 Revision 4 (v4): SI-13 b
NIST: NIST SP 800-53A (v1): SI-13.1 (iii)

---

**CCI:** CCI-002762 **Status:** draft

**Contributor:** DISA FSO **Published** 2013-07-11

**Date:**

**Definition:** The organization defines the mean time to failure (MTTF) substitution criteria to be employed as a means to determine the need to exchange active and standby components.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-13 b

---

**CCI:** CCI-002763 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization provides a means to exchange active and standby components in accordance with the organization-defined mean time to failure (MTTF) substitution criteria.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-13 b

---

**CCI:** CCI-001319 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization takes information system components out of service by transferring component responsibilities to a substitute component no later than an organization-defined fraction or percentage of mean time to failure (MTTF).

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SI-13 (1)
NIST: NIST SP 800-53 Revision 4 (v4): SI-13 (1)
NIST: NIST SP 800-53A (v1): SI-13 (1).1 (ii)

---

**CCI:** CCI-001320 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization defines the maximum fraction or percentage of mean time to failure (MTTF) used to determine when information system components are taken out of service by transferring component responsibilities to substitute components.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SI-13 (1)
NIST: NIST SP 800-53 Revision 4 (v4): SI-13 (1)
NIST: NIST SP 800-53A (v1): SI-13 (1).1 (i)

---

**CCI:** CCI-001323 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization manually initiates a transfer between active and standby information system components in accordance with organization-defined frequency if the mean time to failure (MTTF) exceeds an organization-defined time period.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SI-13 (3)
NIST: NIST SP 800-53 Revision 4 (v4): SI-13 (3)

NIST: NIST SP 800-53A (v1): SI-13 (3).1 (iii)

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-001324 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |

**Definition:** The organization defines the minimum frequency at which the organization manually initiates a transfer between active and standby information system components if the mean time to failure (MTTF) exceeds the organization-defined time period.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SI-13 (3)
NIST: NIST SP 800-53 Revision 4 (v4): SI-13 (3)
NIST: NIST SP 800-53A (v1): SI-13 (3).1 (i)

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-001325 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |

**Definition:** The organization defines a time period that the mean time to failure (MTTF) must exceed before the organization manually initiates a transfer between active and standby information system components.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SI-13 (3)
NIST: NIST SP 800-53 Revision 4 (v4): SI-13 (3)
NIST: NIST SP 800-53A (v1): SI-13 (3).1 (ii)

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-001326 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |

**Definition:** The organization, if information system component failures are detected, ensures standby components are successfully and transparently installed within an organization-defined time period.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SI-13 (4) (a)
NIST: NIST SP 800-53 Revision 4 (v4): SI-13 (4) (a)
NIST: NIST SP 800-53A (v1): SI-13 (4).1 (iii)

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-001327 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |

**Definition:** The organization defines a time period for a standby information system component to be successfully and transparently installed for the information system component that has failed.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SI-13 (4) (a)
NIST: NIST SP 800-53 Revision 4 (v4): SI-13 (4) (a)
NIST: NIST SP 800-53A (v1): SI-13 (4).1 (i)

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001328 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization, if an information system component failure is detected, activates an organization-defined alarm and/or automatically shuts down the information system. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): SI-13 (4) (b)<br>NIST: NIST SP 800-53 Revision 4 (v4): SI-13 (4) (b)<br>NIST: NIST SP 800-53A (v1): SI-13 (4).1 (iii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001329 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization defines the alarm to be activated when an information system component failure is detected. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SI-13 (4) (b)<br>NIST: NIST SP 800-53 Revision 4 (v4): SI-13 (4) (b)<br>NIST: NIST SP 800-53A (v1): SI-13 (4).1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000558 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization defines the real-time or near-real-time failover capability to be provided for the information system. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CP-10 (5)<br>NIST: NIST SP 800-53 Revision 4 (v4): SI-13 (5)<br>NIST: NIST SP 800-53A (v1): CP-10 (5).1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000559 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization provides real-time or near-real-time organization-defined failover capability for the information system. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CP-10 (5)<br>NIST: NIST SP 800-53 Revision 4 (v4): SI-13 (5)<br>NIST: NIST SP 800-53A (v1): CP-10 (5).1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002764 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |

**Definition:** The organization defines non-persistent information system components and services to be implemented.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-14

---

**CCI:** CCI-002765 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization defines the frequency at which it will terminate organization-defined non-persistent information system components and services.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-14

---

**CCI:** CCI-002766 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization implements organization-defined non-persistence information system components and services that are initiated in a known state.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-14

---

**CCI:** CCI-002767 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization implements organization-defined non-persistence information system components and services that are terminated upon end of session of use and/or periodically at an organization-defined frequency.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-14

---

**CCI:** CCI-002768 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization defines the trusted sources from which it obtains software and data employed during the refreshing of non-persistent information system components and services.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-14 (1)

---

**CCI:** CCI-002769 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization ensures that software and data employed during non-persistent information system component and service refreshes are obtained from organization-defined trusted sources.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-14 (1)

---

**CCI:** CCI-002770 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization defines the software programs and/or applications from which the information system is to validate the information output to ensure the information is consistent with expected content.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-15

---

**CCI:** CCI-002771 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The information system validates information output from organization-defined software programs and/or applications to ensure that the information is consistent with the expected content.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-15

---

**CCI:** CCI-002772 **Status:** deprecated

**Contributor:** DISA FSO **Published Date:** 2013-07-11

**Definition:** The organization defines the security safeguards to be implemented to protect the information system's memory from unauthorized code execution.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-15

---

**CCI:** CCI-002823 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-12

**Definition:** The organization defines the security safeguards to be implemented to protect the information system's memory from unauthorized code execution.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-16

---

**CCI:** CCI-002824 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-07-12

**Definition:** The information system implements organization-defined security safeguards to protect its memory from unauthorized code execution.

**Type:** technical

**References:** NIST: NIST SP 800-53 Revision 4 (v4): SI-16

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002773 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The organization defines the fail-safe procedures to be implemented by the information system when organization-defined failure conditions occur. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-17 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002774 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The organization defines the failure conditions which, when they occur, will result in the information system implementing organization-defined fail-safe procedures. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-17 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-002775 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-07-11 |
| **Definition:** | The information system implements organization-defined fail-safe procedures when organization-defined failure conditions occur. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): SI-17 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003556 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-08 |
| **Definition:** | The organization provides effective notice to the public regarding its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of personally identifiable information (PII). | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): TR-1 a | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003557 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-08 |
| **Definition:** | The organization provides effective notice to individuals regarding its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of personally identifiable information (PII). | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): TR-1 a | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003558 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-08 |

**Definition:** The organization provides effective notice to the public regarding its authority for collecting personally identifiable information (PII).

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): TR-1 a

---

**CCI:** CCI-003559 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-08

**Definition:** The organization provides effective notice to individuals regarding its authority for collecting personally identifiable information (PII).

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): TR-1 a

---

**CCI:** CCI-003560 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-08

**Definition:** The organization provides effective notice to the public regarding the choices, if any, individuals may have regarding how the organization uses personally identifiable information (PII).

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): TR-1 a

---

**CCI:** CCI-003561 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-08

**Definition:** The organization provides effective notice to individuals regarding the choices, if any, individuals may have regarding how the organization uses personally identifiable information (PII).

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): TR-1 a

---

**CCI:** CCI-003562 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-08

**Definition:** The organization provides effective notice to the public regarding the consequences of exercising or not exercising the choices regarding how the organization uses personally identifiable information (PII).

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): TR-1 a

---

**CCI:** CCI-003563 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-08

**Definition:** The organization provides effective notice to individuals regarding the consequences of exercising or not exercising the choices regarding how the organization uses personally identifiable information (PII).

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): TR-1 a

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-003564 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-08 |

**Definition:** The organization provides effective notice to the public regarding the ability to access personally identifiable information (PII).

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): TR-1 a

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-003565 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-08 |

**Definition:** The organization provides effective notice to individuals regarding the ability to access personally identifiable information (PII).

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): TR-1 a

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-003566 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-08 |

**Definition:** The organization provides effective notice to the public regarding the ability to have personally identifiable information (PII) amended or corrected if necessary.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): TR-1 a

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-003567 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-08 |

**Definition:** The organization provides effective notice to individuals regarding the ability to have personally identifiable information (PII) amended or corrected if necessary.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): TR-1 a

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-003568 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-08 |

**Definition:** The organization describes the personally identifiable information (PII) the organization collects.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): TR-1 b

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-003569 | **Status:** | draft |

**Contributor:** DISA FSO **Published Date:** 2013-11-08

**Definition:** The organization describes the purpose(s) for which it collects the personally identifiable information (PII).

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): TR-1 b

---

**CCI:** CCI-003570 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-08

**Definition:** The organization describes how the organization uses personally identifiable information (PII) internally.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): TR-1 b

---

**CCI:** CCI-003571 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-08

**Definition:** The organization describes whether the organization shares personally identifiable information (PII) with external entities.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): TR-1 b

---

**CCI:** CCI-003572 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-08

**Definition:** The organization describes the categories of those external entities with whom personally identifiable information (PII) is shared.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): TR-1 b

---

**CCI:** CCI-003573 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-08

**Definition:** The organization describes the purposes for sharing personally identifiable information (PII) with external entities.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): TR-1 b

---

**CCI:** CCI-003574 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-08

**Definition:** The organization describes whether individuals have the ability to consent to specific uses or sharing of personally identifiable information (PII).

**Type:** policy

| | |
|---|---|
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): TR-1 b |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003575 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-08 |
| **Definition:** | The organization describes how individuals may exercise their consent regarding specific uses or sharing of personally identifiable information (PII). | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): TR-1 b | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003576 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-08 |
| **Definition:** | The organization describes how individuals may obtain access to personally identifiable information (PII). | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): TR-1 b | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003577 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-08 |
| **Definition:** | The organization describes how the personally identifiable information (PII) will be protected. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): TR-1 b | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003578 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-08 |
| **Definition:** | The organization revises its public notices to reflect changes in practice or policy that affect personally identifiable information (PII), before or as soon as practicable after the change. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): TR-1 c | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003579 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-08 |
| **Definition:** | The organization revises its public notices to reflect changes in practice or policy that impact privacy, before or as soon as practicable after the change. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 Revision 4 (v4): TR-1 c | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003580 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-08 |

**Definition:** The organization provides real-time notice and/or layered notice when it collects personally identifiable information (PII).

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): TR-1 (1)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003581 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-08 |

**Definition:** The organization publishes System of Records Notices (SORNs) in the Federal Register, subject to required oversight processes, for systems containing personally identifiable information (PII).

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): TR-2 a

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003582 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-08 |

**Definition:** The organization keeps System of Records Notices (SORNs) current.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): TR-2 b

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003583 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-08 |

**Definition:** The organization includes Privacy Act Statements on its forms that collect personally identifiable information (PII), or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): TR-2 c

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003584 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-08 |

**Definition:** The organization publishes System of Records Notices (SORNs) on its public website.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): TR-2 (1)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003585 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-08 |

**Definition:** The organization ensures the public has access to information about its privacy activities.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): TR-3 a

---

**CCI:** CCI-003586 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-11-08
**Definition:** The organization ensures the public is able to communicate with its Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO).
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): TR-3 a

---

**CCI:** CCI-003587 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-11-08
**Definition:** The organization ensures its privacy practices are publicly available through organizational websites or otherwise.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): TR-3 b

---

**CCI:** CCI-003588 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-11-08
**Definition:** The organization uses personally identifiable information (PII) internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): UL-1

---

**CCI:** CCI-003589 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-11-08
**Definition:** The organization shares personally identifiable information (PII) externally, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or for a purpose that is compatible with those purposes.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): UL-2 a

---

**CCI:** CCI-003590 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2013-11-08
**Definition:** The organization, where appropriate, enters into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements, with third parties that specifically describe the personally identifiable information (PII) covered.
**Type:** policy
**References:** NIST: NIST SP 800-53 Revision 4 (v4): UL-2 b

---

**CCI:** CCI-003591 **Status:** draft
**Contributor:** DISA FSO **Published** 2013-11-08

**Date:**

**Definition:** The organization, where appropriate, enters into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements, with third parties that specifically enumerate the purposes for which the personally identifiable information (PII) may be used.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): UL-2 b

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003592 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-08 |

**Definition:** The organization monitors its staff on the authorized sharing of personally identifiable information (PII) with third parties.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): UL-2 c

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003593 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-08 |

**Definition:** The organization audits its staff on the authorized sharing of personally identifiable information (PII) with third parties.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): UL-2 c

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003594 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-08 |

**Definition:** The organization trains its staff on the authorized sharing of personally identifiable information (PII) with third parties.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): UL-2 c

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003595 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-08 |

**Definition:** The organization trains its staff on the consequences of unauthorized use or sharing of personally identifiable information (PII).

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): UL-2 c

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-003596 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2013-11-08 |

**Definition:** The organization evaluates any proposed new instances of sharing personally identifiable information (PII) with third parties to assess whether the sharing is authorized.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): UL-2 d

---

**CCI:** CCI-003597 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2013-11-08

**Definition:** The organization evaluates any proposed new instances of sharing personally identifiable information (PII) with third parties to assess whether additional or new public notice is required.

**Type:** policy

**References:** NIST: NIST SP 800-53 Revision 4 (v4): UL-2 d

---

**CCI:** CCI-000062 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-05-19

**Definition:** The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission/business objectives.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-14 (1)
NIST: NIST SP 800-53A (v1): AC-14 (1).1

---

**CCI:** CCI-001426 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-25

**Definition:** The information system maintains the binding of security attributes to information with sufficient assurance that the information--attribute association can be used as the basis for automated policy actions.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AC-16 (3)
NIST: NIST SP 800-53A (v1): AC-16 (3).1

---

**CCI:** CCI-001427 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-25

**Definition:** The information system allows authorized users to associate security attributes with information.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AC-16 (4)
NIST: NIST SP 800-53A (v1): AC-16 (4).1 (ii)

---

**CCI:** CCI-001396 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization defines security attributes for which the information system supports and maintains the bindings for information in storage.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-16
NIST: NIST SP 800-53A (v1): AC-16.1 (i)

---

**CCI:** CCI-001397 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization defines security attributes for which the information system supports and maintains the bindings for information in process.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-16
NIST: NIST SP 800-53A (v1): AC-16.1 (i)

---

**CCI:** CCI-001398 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization defines security attributes for which the information system supports and maintains the bindings for information in transmission.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-16
NIST: NIST SP 800-53A (v1): AC-16.1 (i)

---

**CCI:** CCI-001399 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The information system supports and maintains the binding of organization-defined security attributes to information in storage.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AC-16
NIST: NIST SP 800-53A (v1): AC-16.1 (ii)

---

**CCI:** CCI-001400 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The information system supports and maintains the binding of organization-defined security attributes to information in process.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AC-16
NIST: NIST SP 800-53A (v1): AC-16.1 (ii)

---

**CCI:** CCI-001401 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The information system supports and maintains the binding of organization-defined security

| | | | |
|---|---|---|---|
| | attributes to information in transmission. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-16<br>NIST: NIST SP 800-53A (v1): AC-16.1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001562 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-11 |
| **Definition:** | The organization defines the appropriate action(s) to be taken if an unauthorized remote connection is discovered. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-17 (5)<br>NIST: NIST SP 800-53A (v1): AC-17 (5).1 (iii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000064 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-05-19 |
| **Definition:** | The organization establishes usage restrictions and implementation guidance for each allowed remote access method. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-17 b<br>NIST: NIST SP 800-53A (v1): AC-17.1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000066 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-14 |
| **Definition:** | The organization enforces requirements for remote connections to the information system. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-17 e<br>NIST: NIST SP 800-53A (v1): AC-17.1 (v) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000071 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-05-19 |
| **Definition:** | The organization monitors for unauthorized remote connections to the information system on an organization-defined frequency. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-17 (5)<br>NIST: NIST SP 800-53A (v1): AC-17 (5).1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000079 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-14 |
| **Definition:** | The organization ensures that remote sessions for accessing an organization-defined list of | | |

security functions and security-relevant information employ organization-defined additional security measures.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-17 (7)
NIST: NIST SP 800-53A (v1): AC-17 (7).1 (iii)

---

**CCI:** CCI-001431 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-25

**Definition:** The organization defines a frequency for monitoring for unauthorized remote connections to the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-17 (5)
NIST: NIST SP 800-53A (v1): AC-17 (5).1 (i)

---

**CCI:** CCI-001432 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-25

**Definition:** The organization takes appropriate action if an unauthorized remote connection to the information system is discovered.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-17 (5)
NIST: NIST SP 800-53A (v1): AC-17 (5).1 (iv)

---

**CCI:** CCI-001433 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-25

**Definition:** The organization defines a list of security functions and security-relevant information that for remote access sessions have organization-defined security measures employed and are audited.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-17 (7)
NIST: NIST SP 800-53A (v1): AC-17 (7).1 (i)

---

**CCI:** CCI-001434 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-25

**Definition:** The organization defines additional security measures to be employed when an organization-defined list of security functions and security-relevant information is accessed remotely.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-17 (7)
NIST: NIST SP 800-53A (v1): AC-17 (7).1 (ii)

---

**CCI:** CCI-001435 **Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2009-09-25

**Definition:** The organization defines networking protocols within the information system deemed to be nonsecure.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-17 (8)

NIST: NIST SP 800-53A (v1): AC-17 (8).1 (i)

---

**CCI:** CCI-001436

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2009-09-25

**Definition:** The organization disables organization-defined networking protocols within the information system deemed to be nonsecure except for explicitly identified components in support of specific operational requirements.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AC-17 (8)

NIST: NIST SP 800-53A (v1): AC-17 (8).1 (ii)

---

**CCI:** CCI-001437

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2009-09-25

**Definition:** The organization documents the rationale for the execution of privileged commands and access to security-relevant information in the security plan for the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-17 (4)

NIST: NIST SP 800-53A (v1): AC-17 (4).1 (ii)

---

**CCI:** CCI-001454

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2009-09-29

**Definition:** The organization ensures that remote sessions for accessing an organization-defined list of security functions and security-relevant information are audited.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AC-17 (7)

NIST: NIST SP 800-53A (v1): AC-17 (7).1 (iv)

---

**CCI:** CCI-001455

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2009-09-29

**Definition:** The organization explicitly identifies components needed in support of specific operational requirements.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-17 (8)

NIST: NIST SP 800-53A (v1): AC-17 (8).1 (ii)

---

**CCI:** CCI-001402 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-22
**Definition:** The organization monitors for unauthorized remote access to the information system.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): AC-17 c
NIST: NIST SP 800-53A (v1): AC-17.1 (iii)

---

**CCI:** CCI-001563 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2010-05-11
**Definition:** The organization defines the appropriate action(s) to be taken if an unauthorized wireless connection is discovered.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): AC-18 (2)
NIST: NIST SP 800-53A (v1): AC-18 (2).1 (iii)

---

**CCI:** CCI-001440 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-25
**Definition:** The organization monitors for unauthorized wireless access to the information system.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): AC-18 b
NIST: NIST SP 800-53A (v1): AC-18.1 (ii)

---

**CCI:** CCI-001442 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-25
**Definition:** The organization enforces requirements for wireless connections to the information system.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): AC-18 d
NIST: NIST SP 800-53A (v1): AC-18.1 (iv)

---

**CCI:** CCI-001445 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-25
**Definition:** The organization monitors for unauthorized wireless connections to the information system on an organization-defined frequency.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): AC-18 (2)
NIST: NIST SP 800-53A (v1): AC-18 (2).1 (ii)

---

**CCI:** CCI-001446 **Status:** draft
**Contributor:** DISA FSO **Published** 2009-09-25

| | | | |
|---|---|---|---|
| | | **Date:** | |
| **Definition:** | The organization scans for unauthorized wireless access points on an organization-defined frequency. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-18 (2)<br>NIST: NIST SP 800-53A (v1): AC-18 (2).1 (ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001447 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-25 |
| **Definition:** | The organization defines a frequency of monitoring for unauthorized wireless connections to information system, including scans for unauthorized wireless access points. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-18 (2)<br>NIST: NIST SP 800-53A (v1): AC-18 (2).1 (i) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001448 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-25 |
| **Definition:** | The organization takes appropriate action if an unauthorized wireless connection is discovered. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-18 (2)<br>NIST: NIST SP 800-53A (v1): AC-18 (2).1 (iv) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001450 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-25 |
| **Definition:** | The organization does not allow users to independently configure wireless networking capabilities. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-18 (4)<br>NIST: NIST SP 800-53A (v1): AC-18 (4).1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000085 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-05-19 |
| **Definition:** | The organization monitors for unauthorized connections of mobile devices to organizational information systems. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-19 c<br>NIST: NIST SP 800-53A (v1): AC-19.1 (iii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000086 | **Status:** | draft |

| | | | |
|---|---|---|---|
| **Contributor:** | DISA FSO | **Published Date:** | 2009-05-19 |
| **Definition:** | The organization enforces requirements for the connection of mobile devices to organizational information systems. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-19 d<br>NIST: NIST SP 800-53A (v1): AC-19.1 (iv) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000087 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-05-19 |
| **Definition:** | The organization disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-19 e<br>NIST: NIST SP 800-53A (v1): AC-19.1 (v) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000088 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-14 |
| **Definition:** | The organization issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-19 f<br>NIST: NIST SP 800-53A (v1): AC-19.1 (vi) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000089 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-14 |
| **Definition:** | The organization applies organization-defined inspection and preventative measures to mobile devices returning from locations that the organization deems to be of significant risk in accordance with organizational policies and procedures. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-19 g<br>NIST: NIST SP 800-53A (v1): AC-19.1 (viii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000090 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-05-19 |
| **Definition:** | The organization restricts the use of writable, removable media in organizational information systems. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-19 (1)<br>NIST: NIST SP 800-53A (v1): AC-19 (1).1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000091 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-05-19 |
| **Definition:** | The organization prohibits the use of personally-owned, removable media in organizational information systems. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-19 (2)<br>NIST: NIST SP 800-53A (v1): AC-19 (2).1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000092 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-05-19 |
| **Definition:** | The organization prohibits the use of removable media in organizational information systems when the media has no identifiable owner. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-19 (3)<br>NIST: NIST SP 800-53A (v1): AC-19 (3).1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001456 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-29 |
| **Definition:** | The organization defines locations that the organization deems to be of significant risk in accordance with organizational policies and procedures. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-19 f<br>NIST: NIST SP 800-53A (v1): AC-19.1 (vi) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001457 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-29 |
| **Definition:** | The organization defines inspection and preventative measures to be applied on mobile devices returning from locations that the organization deems to be of significant risk in accordance with organizational policies and procedures. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-19 g<br>NIST: NIST SP 800-53A (v1): AC-19.1 (vii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000007 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-05-13 |
| **Definition:** | The organization manages information system accounts by identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary). | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-2 a | | |

NIST: NIST SP 800-53A (v1): AC-2.1 (i)

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000009 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-05-13 |
| **Definition:** | The organization manages information system accounts by identifying authorized users of the information system and specifying access privileges. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-2 c<br>NIST: NIST SP 800-53A (v1): AC-2.1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000013 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-14 |
| **Definition:** | The organization manages information system accounts by notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-2 g<br>NIST: NIST SP 800-53A (v1): AC-2.1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000014 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-14 |
| **Definition:** | The organization manages information system accounts by granting access to the system based on a valid access authorization; intended system usage; and other attributes as required by the organization or associated missions/business functions. | | |
| **Type:** | policy | | |
| **Parameter:** | Organizational Policy identifying the process for user accounts. | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-2 i<br>NIST: NIST SP 800-53A (v1): AC-2.1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000020 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-14 |
| **Definition:** | The information system dynamically manages user privileges and associated access authorizations. | | |
| **Type:** | technical | | |
| **Parameter:** | TBD | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-2 (6)<br>NIST: NIST SP 800-53A (v1): AC-2 (6).1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000237 | **Status:** | draft |

**Contributor:** DISA FSO **Published Date:** 2009-06-23

**Definition:** The organization manages information system accounts by specifically authorizing and monitoring the use of guest/anonymous accounts and temporary accounts.

**Type:** policy

**Parameter:** Procedures for the monitoring of assigned guest/anonymous accounts.

**References:** NIST: NIST SP 800-53 (v3): AC-2 f
NIST: NIST SP 800-53A (v1): AC-2.1 (i)

---

**CCI:** CCI-000208 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-14

**Definition:** The organization determines normal time-of-day and duration usage for information system accounts.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-2 (5) (b)
NIST: NIST SP 800-53A (v1): AC-2 (5).1 (iii)

---

**CCI:** CCI-001354 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization manages information system accounts by deactivating temporary accounts that are no longer required.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-2 h
NIST: NIST SP 800-53A (v1): AC-2.1 (i)

---

**CCI:** CCI-001355 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization manages information system accounts by deactivating accounts of terminated or transferred users.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-2 h
NIST: NIST SP 800-53A (v1): AC-2.1 (i)

---

**CCI:** CCI-001356 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization monitors for atypical usage of information system accounts.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AC-2 (5) (c)
NIST: NIST SP 800-53A (v1): AC-2 (5).1 (iv)

---

**CCI:** CCI-001357 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization reports atypical usage to designated organizational officials.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-2 (5) (d)

NIST: NIST SP 800-53A (v1): AC-2 (5).1 (v)

---

**CCI:** CCI-001359 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization tracks privileged role assignments.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-2 (7) (b)

NIST: NIST SP 800-53A (v1): AC-2 (7).1 (ii)

---

**CCI:** CCI-000094 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-05-19

**Definition:** The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to process organization-controlled information using the external information systems.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-20 b

NIST: NIST SP 800-53A (v1): AC-20.1

---

**CCI:** CCI-000095 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-05-19

**Definition:** The organization prohibits authorized individuals from using an external information system to access the information system except in situations where the organization can verify the implementation of required security controls on the external system as specified in the organization's information security policy and security plan.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-20 (1) (a)

NIST: NIST SP 800-53A (v1): AC-20 (1).1

---

**CCI:** CCI-000096 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-05-19

**Definition:** The organization prohibits authorized individuals from using an external information system to access the information system or to process, store, or transmit organization-controlled information except in situations where the organization has approved information system connection or processing agreements with the organizational entity hosting the external information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-20 (1) (b)<br>NIST: NIST SP 800-53A (v1): AC-20 (1).1

---

**CCI:** CCI-001465 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-29

**Definition:** The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to store organization-controlled information using the external information systems.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-20 b<br>NIST: NIST SP 800-53A (v1): AC-20.1

---

**CCI:** CCI-001466 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-29

**Definition:** The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to transmit organization-controlled information using the external information systems.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-20 b<br>NIST: NIST SP 800-53A (v1): AC-20.1

---

**CCI:** CCI-001467 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-29

**Definition:** The organization prohibits authorized individuals from using an external information system to process organization-controlled information except in situations where the organization can verify the implementation of required security controls on the external system as specified in the organization's information security policy and security plan.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-20 (1) (a)<br>NIST: NIST SP 800-53A (v1): AC-20 (1).1

---

**CCI:** CCI-001468 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-29

**Definition:** The organization prohibits authorized individuals from using an external information system to store organization-controlled information except in situations where the organization can verify the implementation of required security controls on the external system as specified in the organization's information security policy and security plan.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-20 (1) (a)
NIST: NIST SP 800-53A (v1): AC-20 (1).1

---

**CCI:** CCI-001469 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-29

**Definition:** The organization prohibits authorized individuals from using an external information system to transmit organization-controlled information except in situations where the organization can verify the implementation of required security controls on the external system as specified in the organization's information security policy and security plan.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-20 (1) (a)
NIST: NIST SP 800-53A (v1): AC-20 (1).1

---

**CCI:** CCI-000022 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-05-13

**Definition:** The information system enforces one or more organization-defined nondiscretionary access control policies over an organization-defined set of users and resources.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AC-3 (3) (a)
NIST: NIST SP 800-53A (v1): AC-3 (3).1 (iii)

---

**CCI:** CCI-000214 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-14

**Definition:** The organization establishes a Discretionary Access Control (DAC) policy that limits propagation of access rights.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-3 (4) (b)
NIST: NIST SP 800-53A (v1): AC-3 (4).1

---

**CCI:** CCI-000215 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-14

**Definition:** The organization establishes a Discretionary Access Control (DAC) policy that includes or excludes access to the granularity of a single user.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-3 (4) (c)
NIST: NIST SP 800-53A (v1): AC-3 (4).1

---

**CCI:** CCI-001409 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-24

**Definition:** The organization defines nondiscretionary access control policies to be enforced over the organization-defined set of users and resources, where the rule set for each policy specifies access control information employed by the policy rule set (e.g., position, nationality, age, project, time of day) and required relationships among the access control information to permit access.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-3 (3)
NIST: NIST SP 800-53A (v1): AC-3 (3).1 (ii)

---

**CCI:** CCI-001410 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-24

**Definition:** The organization defines the set of users and resources over which the information system is to enforce nondiscretionary access control policies.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-3 (3)
NIST: NIST SP 800-53A (v1): AC-3 (3).1 (i)

---

**CCI:** CCI-001412 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-24

**Definition:** The organization encrypts or stores off-line, in a secure location, organization-defined user information.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-3 (6)
NIST: NIST SP 800-53A (v1): AC-3 (6).1 (ii)

---

**CCI:** CCI-001413 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-24

**Definition:** The organization encrypts or stores off-line, in a secure location, organization-defined system information.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-3 (6)
NIST: NIST SP 800-53A (v1): AC-3 (6).1 (ii)

---

**CCI:** CCI-001362 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The information system enforces a Discretionary Access Control (DAC) policy that allows users to specify and control sharing by named individuals or groups of individuals, or by both.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AC-3 (4)
NIST: NIST SP 800-53A (v1): AC-3 (4).1

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001363 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization establishes a Discretionary Access Control (DAC) policy that allows users to specify and control sharing by named individuals or groups of individuals, or by both. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-3 (4) (a) | | |
| | NIST: NIST SP 800-53A (v1): AC-3 (4).1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001366 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization defines user information to be encrypted or stored off-line in a secure location. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-3 (6) | | |
| | NIST: NIST SP 800-53A (v1): AC-3 (6).1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001367 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization defines system information to be encrypted or stored off-line in a secure location. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-3 (6) | | |
| | NIST: NIST SP 800-53A (v1): AC-3 (6).1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001693 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2011-10-07 |
| **Definition:** | The information system enforces a Discretionary Access Control (DAC) policy that limits propagation of access rights. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-3 (4) | | |
| | NIST: NIST SP 800-53A (v1): AC-3 (4).1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001694 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2011-10-07 |
| **Definition:** | The information system enforces a Discretionary Access Control (DAC) policy that includes or excludes access to the granularity of a single user. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-3 (4) | | |

NIST: NIST SP 800-53A (v1): AC-3 (4).1

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001552 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-11 |
| **Definition:** | The organization defines policy that allows or disallows information flows based on changing conditions or operational considerations. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-4 (3)<br>NIST: NIST SP 800-53A (v1): AC-4 (3).1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001555 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-11 |
| **Definition:** | The information system uniquely identifies destination domains for information transfer. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-4 (17) (a)<br>NIST: NIST SP 800-53A (v1): AC-4 (17).1 (iii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001556 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-11 |
| **Definition:** | The information system uniquely authenticates destination domains for information transfer. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-4 (17) (a)<br>NIST: NIST SP 800-53A (v1): AC-4 (17).1 (iv) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001557 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-11 |
| **Definition:** | The information system tracks problems associated with the information transfer. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-4 (17) c<br>NIST: NIST SP 800-53A (v1): AC-4 (17).1 (vii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000025 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-14 |
| **Definition:** | The information system enforces information flow control using explicit security attributes on information, source, and destination objects as a basis for flow control decisions. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-4 (1)<br>NIST: NIST SP 800-53A (v1): AC-4 (1).1 | | |

**CCI:** CCI-000033
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2009-05-13
**Definition:** The information system enforces the use of human review for organization-defined security policy filters when the system is not capable of making an information flow control decision.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): AC-4 (9)
NIST: NIST SP 800-53A (v1): AC-4 (9).1 (ii)

---

**CCI:** CCI-000218
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2009-09-14
**Definition:** The information system, when transferring information between different security domains, identifies information flows by data type specification and usage.
**Type:** technical
**References:** NIST: NIST SP 800-53 (v3): AC-4 (12)
NIST: NIST SP 800-53A (v1): AC-4 (12).1

---

**CCI:** CCI-000221
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2009-09-14
**Definition:** The information system enforces security policies regarding information on interconnected systems.
**Type:** technical
**References:** NIST: NIST SP 800-53 (v3): AC-4 (16)
NIST: NIST SP 800-53A (v1): AC-4 (16).1

---

**CCI:** CCI-000223
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2009-09-14
**Definition:** The information system binds security attributes to information to facilitate information flow policy enforcement.
**Type:** technical
**References:** NIST: NIST SP 800-53 (v3): AC-4 (17) (b)
NIST: NIST SP 800-53A (v1): AC-4 (17).1 (v)

---

**CCI:** CCI-000224
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2009-09-14
**Definition:** The information system tracks problems associated with the security attribute binding.
**Type:** technical
**References:** NIST: NIST SP 800-53 (v3): AC-4 (17) (c)
NIST: NIST SP 800-53A (v1): AC-4 (17).1 (vi)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001418 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-24 |
| **Definition:** | The organization defines security policy filters for which the information system enforces the use of human review. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-4 (9)<br>NIST: NIST SP 800-53A (v1): AC-4 (9).1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001376 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The information system uniquely identifies source domains for information transfer. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-4 (17) (a)<br>NIST: NIST SP 800-53A (v1): AC-4 (17).1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001377 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The information system uniquely authenticates source domains for information transfer. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-4 (17) (a)<br>NIST: NIST SP 800-53A (v1): AC-4 (17).1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000037 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-14 |
| **Definition:** | The organization implements separation of duties through assigned information system access authorizations. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-5 c<br>NIST: NIST SP 800-53A (v1): AC-5.1 (iii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000038 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-05-19 |
| **Definition:** | The organization explicitly authorizes access to organization-defined security functions and security-relevant information. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-6 (1)<br>NIST: NIST SP 800-53A (v1): AC-6 (1).1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000040 | **Status:** | draft |

| | | | |
|---|---|---|---|
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-14 |
| **Definition:** | The organization audits any use of privileged accounts, or roles, with access to organization-defined security functions or security-relevant information, when accessing other system functions. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-6 (2)<br>NIST: NIST SP 800-53A (v1): AC-6 (2).1 (iii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000226 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-14 |
| **Definition:** | The information system provides the capability for a privileged administrator to configure organization-defined security policy filters to support different security policies. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-6 (4)<br>NIST: NIST SP 800-53A (v1): AC-6 (4).1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001421 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-25 |
| **Definition:** | The organization limits authorization to super user accounts on the information system to designated system administration personnel. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-6 (5)<br>NIST: NIST SP 800-53A (v1): AC-6 (5).1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000045 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-14 |
| **Definition:** | The organization defines in the security plan, explicitly or by reference, the time period for lock out mode or delay period. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-7 b<br>NIST: NIST SP 800-53A (v1): AC-7.1 (iii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000046 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-14 |
| **Definition:** | The organization selects either a lock out mode for the organization-defined time period or delays the next login prompt for the organization-defined delay period for information system responses to consecutive invalid access attempts. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-7 b<br>NIST: NIST SP 800-53A (v1): AC-7.1 (iv) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000047 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-14 |
| **Definition:** | The information system delays next login prompt according to the organization-defined delay algorithm, when the maximum number of unsuccessful attempts is exceeded, automatically locks the account/node for an organization-defined time period or locks the account/node until released by an Administrator IAW organizational policy. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-7 b<br>NIST: NIST SP 800-53A (v1): AC-7.1 (iv) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001452 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-05-25 |
| **Definition:** | The information system enforces the organization-defined time period during which the limit of consecutive invalid access attempts by a user is counted. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-7 a<br>NIST: NIST SP 800-53A (v1): AC-7.1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001382 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization defines the number of consecutive, unsuccessful login attempts to the mobile device. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-7 (2)<br>NIST: NIST SP 800-53A (v1): AC-7 (2).1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001383 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The information system provides additional protection for mobile devices accessed via login by purging information from the device after an organization-defined number of consecutive, unsuccessful login attempts to the mobile device. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): AC-7 (2)<br>NIST: NIST SP 800-53A (v1): AC-7 (2).1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000049 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-05-19 |
| **Definition:** | The organization defines a system use notification message or banner displayed before granting access to the system that provides privacy and security notices consistent with | | |

applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: (i) users are accessing a U.S. Government information system; (ii) system usage may be monitored, recorded, and subject to audit; (iii) unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) use of the system indicates consent to monitoring and recording.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-8 a
NIST: NIST SP 800-53A (v1): AC-8.1 (i)

---

**CCI:** CCI-000051 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-05-19

**Definition:** The organization approves the information system use notification message before its use.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AC-8 a
NIST: NIST SP 800-53A (v1): AC-8.1 (i)

---

**CCI:** CCI-000115 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-14

**Definition:** The organization establishes contact with selected groups and associations within the security community to facilitate ongoing security education and training; to stay up to date with the latest recommended security practices, techniques, and technologies; and to share current security-related information including threats, vulnerabilities, and incidents.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AT-5
NIST: NIST SP 800-53A (v1): AT-5.1

---

**CCI:** CCI-000116 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-14

**Definition:** The organization institutionalizes contact with selected groups and associations within the security community to facilitate ongoing security education and training; to stay up to date with the latest recommended security practices, techniques, and technologies; and to share current security-related information including threats, vulnerabilities, and incidents.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AT-5
NIST: NIST SP 800-53A (v1): AT-5.1

---

**CCI:** CCI-000118 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-05-20

**Definition:** The organization disseminates a formal, documented, audit and accountability policy to elements within the organization having associated audit and accountability roles and responsibilities.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AU-1 a
NIST: NIST SP 800-53A (v1): AU-1.1 (iii)

---

**CCI:** CCI-000121 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-05-20

**Definition:** The organization disseminates formal, documented, procedures to elements within the organization having associated audit and accountability roles and responsibilities.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AU-1 b
NIST: NIST SP 800-53A (v1): AU-1.1 (vi)

---

**CCI:** CCI-001338 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The information system associates the identity of the information producer with the information.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AU-10 (1)
NIST: NIST SP 800-53A (v1): AU-10 (1).1

---

**CCI:** CCI-001339 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The information system validates the binding of the information producer's identity to the information.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AU-10 (2)
NIST: NIST SP 800-53A (v1): AU-10 (2).1

---

**CCI:** CCI-001342 **Status:** deprecated

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization employs either FIPS-validated or NSA-approved cryptography to implement digital signatures.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AU-10 (5)
NIST: NIST SP 800-53A (v1): AU-10 (5).1

---

**CCI:** CCI-001148 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization employs FIPS-validated or NSA-approved cryptography to implement digital signatures.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SC-13 (4)
NIST: NIST SP 800-53 (v3): AU-10 (5)
NIST: NIST SP 800-53A (v1): SC-13 (4).1
NIST: NIST SP 800-53A (v1): AU-10 (5).1 (ii)

---

**CCI:** CCI-001463 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-29

**Definition:** The information system provides the capability to remotely view/hear all content related to an established user session in real time.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AU-14 b
NIST: NIST SP 800-53A (v1): AU-14.1 (ii)

---

**CCI:** CCI-000128 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-05-20

**Definition:** The organization includes execution of privileged functions in the list of events to be audited by the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AU-2 (4)
NIST: NIST SP 800-53A (v1): AU-2 (4).1

---

**CCI:** CCI-000129 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-15

**Definition:** The organization defines in the auditable events that the information system must be capable of auditing based on a risk assessment and mission/business needs.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AU-2 a
NIST: NIST SP 800-53A (v1): AU-2.1 (ii)

---

**CCI:** CCI-000136 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-05-20

**Definition:** The organization centrally manages the content of audit records generated by organization-defined information system components.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AU-3 (2)
NIST: NIST SP 800-53A (v1): AU-3 (2).1 (ii)

---

**CCI:** CCI-001489 **Status:** draft

| | | | |
|---|---|---|---|
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-29 |
| **Definition:** | The organization defines information system components for which generated audit records are centrally managed by the organization. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): AU-3 (2)<br>NIST: NIST SP 800-53A (v1): AU-3 (2).1 (i) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000137 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-05-20 |
| **Definition:** | The organization allocates audit record storage capacity. | | |
| **Type:** | policy, technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): AU-4<br>NIST: NIST SP 800-53A (v1): AU-4.1 (i) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000138 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-05-20 |
| **Definition:** | The organization configures auditing to reduce the likelihood of storage capacity being exceeded. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): AU-4<br>NIST: NIST SP 800-53A (v1): AU-4.1 (ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001574 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-11 |
| **Definition:** | The information system rejects or delays, as defined by the organization, network traffic which exceed the organization-defined thresholds. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): AU-5 (3)<br>NIST: NIST SP 800-53A (v1): AU-5 (3).1 (iii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000143 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-05-20 |
| **Definition:** | The information system provides a warning when allocated audit record storage volume reaches an organization-defined percentage of maximum audit record storage capacity. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): AU-5 (1)<br>NIST: NIST SP 800-53A (v1): AU-5 (1).1 (ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000144 | **Status:** | draft |

**Contributor:** DISA FSO **Published Date:** 2009-05-20

**Definition:** The information system provides a real-time alert when organization-defined audit failure events occur.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AU-5 (2)
NIST: NIST SP 800-53A (v1): AU-5 (2).1 (ii)

---

**CCI:** CCI-000146 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-05-20

**Definition:** The organization defines the percentage of maximum audit record storage capacity that when exceeded, a warning is provided.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AU-5 (1)
NIST: NIST SP 800-53A (v1): AU-5 (1).1 (i)

---

**CCI:** CCI-001343 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The information system invokes a system shutdown in the event of an audit failure, unless an alternative audit capability exists.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AU-5 (4)
NIST: NIST SP 800-53A (v1): AU-5 (4).1

---

**CCI:** CCI-000150 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-15

**Definition:** The organization adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): AU-6 b
NIST: NIST SP 800-53A (v1): AU-6.2

---

**CCI:** CCI-000152 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-05-22

**Definition:** The information system integrates audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): AU-6 (1)
NIST: NIST SP 800-53A (v1): AU-6 (1).1

**CCI:** CCI-000155 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-15
**Definition:** The organization integrates analysis of audit records with analysis of vulnerability scanning information, performance data, and network monitoring information to further enhance the ability to identify inappropriate or unusual activity.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): AU-6 (5)
NIST: NIST SP 800-53A (v1): AU-6 (5).1

---

**CCI:** CCI-001344 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-22
**Definition:** The organization specifies the permitted actions for each authorized information system process, role, and/or user in the audit and accountability policy.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): AU-6 (7)
NIST: NIST SP 800-53A (v1): AU-6 (7).1

---

**CCI:** CCI-001345 **Status:** deprecated
**Contributor:** DISA FSO **Published Date:** 2009-09-22
**Definition:** The organization employs automated mechanisms to alert security personnel of any organization-defined inappropriate or unusual activities with security implications.
**Type:** technical
**References:** NIST: NIST SP 800-53 (v3): AU-6 (8)
NIST: NIST SP 800-53A (v1): AU-6 (8).1 (ii)

---

**CCI:** CCI-001346 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-22
**Definition:** The organization defines a list of inappropriate or unusual activities with security implications that are to result in alerts to security personnel.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): AU-6 (8)
NIST: NIST SP 800-53A (v1): AU-6 (8).1 (i)

---

**CCI:** CCI-001347 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-22
**Definition:** The organization performs, in a physically dedicated information system, full-text analysis of privileged functions executed.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): AU-6 (9)

NIST: NIST SP 800-53A (v1): AU-6 (9).1

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000156 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-05-22 |
| **Definition:** | The information system provides an audit reduction capability. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): AU-7<br>NIST: NIST SP 800-53A (v1): AU-7.1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000157 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-05-22 |
| **Definition:** | The information system provides a report generation capability. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): AU-7<br>NIST: NIST SP 800-53A (v1): AU-7.1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000160 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-05-22 |
| **Definition:** | The information system synchronizes internal information system clocks on an organization-defined frequency with an organization-defined authoritative time source. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): AU-8 (1)<br>NIST: NIST SP 800-53A (v1): AU-8 (1).1 (iii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001352 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization protects the audit records of non-local accesses to privileged accounts and the execution of privileged functions. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): AU-9 (4) (b)<br>NIST: NIST SP 800-53A (v1): AU-9 (4).1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001579 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-11 |
| **Definition:** | The organization conducts security control assessments using organization-defined forms of testing in accordance with organization-defined frequency and assessment techniques. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CA-2 (2)<br>NIST: NIST SP 800-53A (v1): CA-2 (2).1 (ii) | | |

---

**CCI:** CCI-000249
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2009-09-15
**Definition:** The organizations security assessment plan describes the assessment team.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CA-2 a
NIST: NIST SP 800-53A (v1): CA-2.1 (ii)

---

**CCI:** CCI-000250
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2009-09-15
**Definition:** The organization's security assessment plan describes assessment roles and responsibilities.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CA-2 a
NIST: NIST SP 800-53A (v1): CA-2.1 (ii)

---

**CCI:** CCI-001580
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2010-05-11
**Definition:** The organization identifies connections to external information systems (i.e., information systems outside of the authorization boundary).
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CA-3 b
NIST: NIST SP 800-53A (v1): CA-3.1 (i)

---

**CCI:** CCI-000261
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2009-09-15
**Definition:** The organization monitors the information system connections on an ongoing basis to verify enforcement of security requirements.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CA-3 c
NIST: NIST SP 800-53A (v1): CA-3.1 (iv)

---

**CCI:** CCI-000275
**Status:** draft
**Contributor:** DISA FSO
**Published Date:** 2009-09-15
**Definition:** The organization implements a continuous monitoring program that includes a configuration management process for the information system.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CA-7 a
NIST: NIST SP 800-53A (v1): CA-7.1 (iv)

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-000276 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-15 |

**Definition:** The organization implements a continuous monitoring program that includes a configuration management process for the information system constituent components.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CA-7 a
NIST: NIST SP 800-53A (v1): CA-7.1 (iv)

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-000277 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-15 |

**Definition:** The organization implements a continuous monitoring program that includes a determination of the security impact of changes to the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CA-7 b
NIST: NIST SP 800-53A (v1): CA-7.1 (iv)

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-000278 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-15 |

**Definition:** The organization implements a continuous monitoring program that includes a determination of the security impact of changes to the environment of operation.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CA-7 b
NIST: NIST SP 800-53A (v1): CA-7.1 (iv)

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-000283 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-15 |

**Definition:** The organization plans announced or unannounced assessments (in-depth monitoring, malicious user testing, penetration testing, red team exercises, or other organization-defined forms of security assessment), on an organization-defined frequency, to ensure compliance with all vulnerability mitigation procedures.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CA-7 (2)
NIST: NIST SP 800-53A (v1): CA-7 (2).1 (ii)

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-000284 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-15 |

**Definition:** The organization schedules announced or unannounced assessments (in-depth monitoring, malicious user testing, penetration testing, red team exercises, or other organization-defined forms of security assessment), on an organization-defined frequency, to ensure compliance with all vulnerability mitigation procedures.

| | | | |
|---|---|---|---|
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CA-7 (2)<br>NIST: NIST SP 800-53A (v1): CA-7 (2).1 (ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000285 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-15 |
| **Definition:** | The organization conducts announced or unannounced assessments (in-depth monitoring, malicious user testing, penetration testing, red team exercises, or other organization-defined forms of security assessment), on an organization-defined frequency, to ensure compliance with all vulnerability mitigation procedures. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CA-7 (2)<br>NIST: NIST SP 800-53A (v1): CA-7 (2).1 (ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000288 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |
| **Definition:** | The organization disseminates formal, documented configuration management policy to elements within the organization having associated configuration management roles and responsibilities. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CM-1 a<br>NIST: NIST SP 800-53A (v1): CM-1.1 (iii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000291 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |
| **Definition:** | The organization disseminates formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CM-1 b<br>NIST: NIST SP 800-53A (v1): CM-1.1 (vi) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000305 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |
| **Definition:** | The organization develops a list of software programs not authorized to execute on the information system. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CM-2 (4) (a)<br>NIST: NIST SP 800-53 (v3): CM-7 (2)<br>NIST: NIST SP 800-53A (v1): CM-2 (4).1 (i)<br>NIST: NIST SP 800-53A (v1): CM-7 (2).1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000306 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |
| **Definition:** | The organization maintains the list of software programs not authorized to execute on the information system. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CM-2 (4) (a)<br>NIST: NIST SP 800-53 (v3): CM-7 (2)<br>NIST: NIST SP 800-53A (v1): CM-2 (4).1 (i)<br>NIST: NIST SP 800-53A (v1): CM-7 (2).1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000307 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |
| **Definition:** | The organization employs an allow-all, deny-by-exception authorization policy to identify software allowed to execute on the information system. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CM-2 (4) (b)<br>NIST: NIST SP 800-53A (v1): CM-2 (4).1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000308 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |
| **Definition:** | The organization develops the list of software programs authorized to execute on the information system. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CM-2 (5) (a)<br>NIST: NIST SP 800-53 (v3): CM-7 (2)<br>NIST: NIST SP 800-53A (v1): CM-2 (5).1 (i)<br>NIST: NIST SP 800-53A (v1): CM-7 (2).1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000309 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |
| **Definition:** | The organization maintains the list of software programs authorized to execute on the information system. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CM-2 (5) (a)<br>NIST: NIST SP 800-53 (v3): CM-7 (2)<br>NIST: NIST SP 800-53A (v1): CM-2 (5).1 (i)<br>NIST: NIST SP 800-53A (v1): CM-7 (2).1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000310 | **Status:** | draft |

**Contributor:** DISA FSO **Published Date:** 2009-09-17

**Definition:** The organization employs a deny-all, permit-by-exception authorization policy to identify software allowed to execute on the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-2 (5) (b)

NIST: NIST SP 800-53A (v1): CM-2 (5).1 (ii)

---

**CCI:** CCI-000315 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-17

**Definition:** The organization documents approved configuration-controlled changes to the system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-3 c

NIST: NIST SP 800-53A (v1): CM-3.1 (iii)

---

**CCI:** CCI-000317 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-17

**Definition:** The organization reviews records of configuration-controlled changes to the system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-3 d

NIST: NIST SP 800-53A (v1): CM-3.1 (iv)

---

**CCI:** CCI-001587 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2010-05-12

**Definition:** The organization, when analyzing new software in a separate test environment, looks for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-4 (1)

NIST: NIST SP 800-53A (v1): CM-4 (1).1 (ii)

---

**CCI:** CCI-000334 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization analyzes new software in a separate test environment before installation in an operational environment.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-4 (1)

NIST: NIST SP 800-53A (v1): CM-4 (1).1 (i)

---

**CCI:** CCI-000346 **Status:** draft

**Contributor:** DISA FSO **Published** 2009-09-18

**Date:**

**Definition:** The organization employs automated mechanisms to enforce access restrictions.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): CM-5 (1)
NIST: NIST SP 800-53A (v1): CM-5 (1).1

---

**CCI:** CCI-000347 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization employs automated mechanisms to support auditing of the enforcement actions.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): CM-5 (1)
NIST: NIST SP 800-53A (v1): CM-5 (1).1

---

**CCI:** CCI-000351 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization defines critical software programs that the information system will prevent from being installed if such software programs are not signed with a recognized and approved certificate.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-5 (3)
NIST: NIST SP 800-53A (v1): CM-5 (3).1 (i)

---

**CCI:** CCI-000352 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The information system prevents the installation of organization-defined critical software programs that are not signed with a certificate that is recognized and approved by the organization.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): CM-5 (3)
NIST: NIST SP 800-53A (v1): CM-5 (3).1 (ii)

---

**CCI:** CCI-000355 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization limits information system developer/integrator privileges to change hardware components directly within a production environment.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-5 (5) (a)
NIST: NIST SP 800-53A (v1): CM-5 (5).1 (i)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000356 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |
| **Definition:** | The organization limits information system developer/integrator privileges to change software components directly within a production environment. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CM-5 (5) (a)<br>NIST: NIST SP 800-53A (v1): CM-5 (5).1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000357 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |
| **Definition:** | The organization limits information system developer/integrator privileges to change firmware components directly within a production environment. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CM-5 (5) (a)<br>NIST: NIST SP 800-53A (v1): CM-5 (5).1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000358 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |
| **Definition:** | The organization limits information system developer/integrator privileges to change system information directly within a production environment. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CM-5 (5) (a)<br>NIST: NIST SP 800-53A (v1): CM-5 (5).1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000359 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |
| **Definition:** | The organization defines the frequency to review information system developer/integrator privileges. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CM-5 (5) (b)<br>NIST: NIST SP 800-53A (v1): CM-5 (5).1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000360 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |
| **Definition:** | The organization defines the frequency to reevaluate information system developer/integrator privileges. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CM-5 (5) (b)<br>NIST: NIST SP 800-53A (v1): CM-5 (5).1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000361 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |
| **Definition:** | The organization reviews information system developer/integrator privileges per organization-defined frequency. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CM-5 (5) (b)<br>NIST: NIST SP 800-53A (v1): CM-5 (5).1 (iii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000362 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |
| **Definition:** | The organization reevaluates information system developer/integrator privileges per organization-defined frequency. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CM-5 (5) (b)<br>NIST: NIST SP 800-53A (v1): CM-5 (5).1 (iii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001500 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-29 |
| **Definition:** | The information system automatically implements organization-defined safeguards and countermeasures if security functions (or mechanisms) are changed inappropriately. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): CM-5 (7)<br>NIST: NIST SP 800-53A (v1): CM-5 (7).1 (ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001501 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-29 |
| **Definition:** | The organization defines safeguards and countermeasures to be employed by the information system if security functions (or mechanisms) are changed inappropriately. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CM-5 (7)<br>NIST: NIST SP 800-53A (v1): CM-5 (7).1 (i) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001589 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-12 |
| **Definition:** | The organization incorporates detection of unauthorized, security-relevant configuration changes into the organization’s incident response capability to ensure they are tracked. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): CM-6 (3)<br>NIST: NIST SP 800-53A (v1): CM-6 (3).1 (ii) | | |

---

**CCI:** CCI-000373 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization defines configuration settings for which unauthorized changes are responded to by automated mechanisms.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-6 (2)

NIST: NIST SP 800-53A (v1): CM-6 (2).1 (i)

---

**CCI:** CCI-000374 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization employs automated mechanisms to respond to unauthorized changes to organization-defined configuration settings.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): CM-6 (2)

NIST: NIST SP 800-53A (v1): CM-6 (2).1 (ii)

---

**CCI:** CCI-000375 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization incorporates detection of unauthorized, security-relevant configuration changes into the organizations incident response capability.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-6 (3)

NIST: NIST SP 800-53A (v1): CM-6 (3).1 (i)

---

**CCI:** CCI-000376 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization ensures unauthorized, security-relevant configuration changes detected are monitored.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-6 (3)

NIST: NIST SP 800-53A (v1): CM-6 (3).1 (ii)

---

**CCI:** CCI-000377 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization ensures unauthorized, security-relevant configuration changes detected are corrected.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-6 (3)

NIST: NIST SP 800-53A (v1): CM-6 (3).1 (ii)

**CCI:** CCI-000378 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-18
**Definition:** The organization ensures unauthorized, security-relevant configuration changes detected are available for historical purposes.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CM-6 (3)
NIST: NIST SP 800-53A (v1): CM-6 (3).1 (ii)

---

**CCI:** CCI-000379 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-18
**Definition:** The information system (including modifications to the baseline configuration) demonstrates conformance to security configuration guidance (i.e., security checklists) prior to being introduced into a production environment.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CM-6 (4)
NIST: NIST SP 800-53A (v1): CM-6 (4).1

---

**CCI:** CCI-001590 **Status:** deprecated
**Contributor:** DISA FSO **Published Date:** 2010-05-12
**Definition:** The organization develops a list of software programs authorized to execute on the information system.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CM-7 (2)
NIST: NIST SP 800-53A (v1): CM-7 (2).1 (i)

---

**CCI:** CCI-001591 **Status:** deprecated
**Contributor:** DISA FSO **Published Date:** 2010-05-12
**Definition:** The organization develops a list of software programs not authorized to execute on the information system.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CM-7 (2)
NIST: NIST SP 800-53A (v1): CM-7 (2).1 (i)

---

**CCI:** CCI-001593 **Status:** deprecated
**Contributor:** DISA FSO **Published Date:** 2010-05-12
**Definition:** The organization maintains a list of software programs authorized to execute on the information system.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CM-7 (2)

NIST: NIST SP 800-53A (v1): CM-7 (2).1 (i)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001594 | **Status:** | deprecated |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-12 |
| **Definition:** | The organization maintains a list of software programs not authorized to execute on the information system. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CM-7 (2) | | |
| | NIST: NIST SP 800-53A (v1): CM-7 (2).1 (i) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001595 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-12 |
| **Definition:** | The organization maintains rules authorizing the terms and conditions of software program usage on the information system. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CM-7 (2) | | |
| | NIST: NIST SP 800-53A (v1): CM-7 (2).1 (i) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000383 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |
| **Definition:** | The organization defines the frequency of information system reviews to identify and eliminate unnecessary functions, ports, protocols and/or services. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CM-7 (1) | | |
| | NIST: NIST SP 800-53A (v1): CM-7 (1).1 (i) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000385 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |
| **Definition:** | The organization reviews the information system per organization-defined frequency to eliminate unnecessary functions, ports, protocols, and/or services. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CM-7 (1) | | |
| | NIST: NIST SP 800-53A (v1): CM-7 (1).1 (ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000386 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |
| **Definition:** | The organization employs automated mechanisms to prevent program execution on the information system in accordance with the organization-defined specifications. | | |
| **Type:** | technical | | |

**References:** NIST: NIST SP 800-53 (v3): CM-7 (2)
NIST: NIST SP 800-53A (v1): CM-7 (2).1 (ii)

---

**CCI:** CCI-000391 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-18
**Definition:** The organization maintains an inventory of information system components that accurately reflects the current information system.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CM-8 a
NIST: NIST SP 800-53A (v1): CM-8.1 (ii)

---

**CCI:** CCI-000394 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-18
**Definition:** The organization maintains an inventory of information system components that is consistent with the authorization boundary of the information system.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CM-8 b
NIST: NIST SP 800-53A (v1): CM-8.1 (ii)

---

**CCI:** CCI-000397 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-18
**Definition:** The organization maintains an inventory of information system components that is at the level of granularity deemed necessary for tracking and reporting.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CM-8 c
NIST: NIST SP 800-53A (v1): CM-8.1 (i)

---

**CCI:** CCI-000401 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-18
**Definition:** The organization maintains an inventory of information system components that includes organization-defined information deemed necessary to achieve effective property accountability.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CM-8 d
NIST: NIST SP 800-53A (v1): CM-8.1 (ii)

---

**CCI:** CCI-000402 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-18
**Definition:** The organization develops an inventory of information system components that is available for review by designated organizational officials.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-8 e<br>NIST: NIST SP 800-53A (v1): CM-8.1 (ii)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000403 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |

**Definition:** The organization documents an inventory of information system components that is available for review by designated organizational officials.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-8 e<br>NIST: NIST SP 800-53A (v1): CM-8.1 (ii)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000404 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |

**Definition:** The organization maintains an inventory of information system components that is available for review by designated organizational officials.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-8 e<br>NIST: NIST SP 800-53A (v1): CM-8.1 (ii)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000405 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |

**Definition:** The organization develops an inventory of information system components that is available for audit by designated organizational officials.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-8 e<br>NIST: NIST SP 800-53A (v1): CM-8.1 (ii)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000406 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |

**Definition:** The organization documents an inventory of information system components that is available for audit by designated organizational officials.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-8 e<br>NIST: NIST SP 800-53A (v1): CM-8.1 (ii)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000407 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |

**Definition:** The organization maintains an inventory of information system components that is available for audit by designated organizational officials.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-8 e
NIST: NIST SP 800-53A (v1): CM-8.1 (ii)

---

**CCI:** CCI-000417 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization disables network access by unauthorized components/devices or notifies designated organizational officials.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): CM-8 (3) (b)
NIST: NIST SP 800-53A (v1): CM-8 (3).1 (iii)

---

**CCI:** CCI-000427 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization develops a configuration management plan for the information system when in the system development life cycle the configuration items are placed under configuration management.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-9 b
NIST: NIST SP 800-53A (v1): CM-9.1 (i)

---

**CCI:** CCI-000428 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization documents a configuration management plan for the information system when in the system development life cycle the configuration items are placed under configuration management.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-9 b
NIST: NIST SP 800-53A (v1): CM-9.1 (i)

---

**CCI:** CCI-000429 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization implements a configuration management plan for the information system when in the system development life cycle the configuration items are placed under configuration management.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-9 b
NIST: NIST SP 800-53A (v1): CM-9.1 (i)

---

**CCI:** CCI-000430 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization develops a configuration management plan for the information system that establishes the means for identifying configuration items throughout the system development life cycle.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-9 c
NIST: NIST SP 800-53A (v1): CM-9.1 (i)

---

**CCI:** CCI-000431 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization documents a configuration management plan for the information system that establishes the means for identifying configuration items throughout the system development life cycle.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-9 c
NIST: NIST SP 800-53A (v1): CM-9.1 (i)

---

**CCI:** CCI-000432 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization implements a configuration management plan for the information system that establishes the means for identifying configuration items throughout the system development life cycle.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-9 c
NIST: NIST SP 800-53A (v1): CM-9.1 (i)

---

**CCI:** CCI-000433 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization develops a configuration management plan for the information system that establishes a process for managing the configuration of the configuration items.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-9 c
NIST: NIST SP 800-53A (v1): CM-9.1 (i)

---

**CCI:** CCI-000434 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization documents a configuration management plan for the information system that establishes a process for managing the configuration of the configuration items.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CM-9 c

| | | | |
|---|---|---|---|
| | NIST: NIST SP 800-53A (v1): CM-9.1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000435 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |
| **Definition:** | The organization implements a configuration management plan for the information system that establishes a process for managing the configuration of the configuration items. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CM-9 c<br>NIST: NIST SP 800-53A (v1): CM-9.1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000554 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization defines in the security plan, explicitly or by reference, the circumstances that can inhibit recovery and reconstitution of the information system to a known state. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CP-10 (3)<br>NIST: NIST SP 800-53A (v1): CP-10 (3).1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000555 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization provides compensating security controls for organization-defined circumstances that can inhibit recovery and reconstitution of the information system to a known state. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CP-10 (3)<br>NIST: NIST SP 800-53A (v1): CP-10 (3).1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000491 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization defines the frequency to exercise the contingency plan for the information system. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): CP-4<br>NIST: NIST SP 800-53A (v1): CP-4.1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000493 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization defines contingency plan exercises to be conducted for the information system. | | |
| **Type:** | policy | | |

**References:** NIST: NIST SP 800-53 (v3): CP-4
NIST: NIST SP 800-53A (v1): CP-4.1 (i)

---

**CCI:** CCI-000495 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization exercises the contingency plan using organization-defined exercises in accordance with organization-defined frequency.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CP-4 a
NIST: NIST SP 800-53A (v1): CP-4.1 (iii)

---

**CCI:** CCI-000499 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization coordinates contingency plan exercises with organizational elements responsible for related plans.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CP-4 (1)
NIST: NIST SP 800-53A (v1): CP-4 (1).1

---

**CCI:** CCI-000501 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization exercises the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site's capabilities to support contingency operations.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CP-4 (2)
NIST: NIST SP 800-53A (v1): CP-4 (2).1

---

**CCI:** CCI-000503 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization employs automated mechanisms to more thoroughly and effectively exercise the contingency plan by providing more complete coverage of contingency issues, selecting more realistic exercise scenarios and environments, and more effectively stressing the information and supported missions.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): CP-4 (3)
NIST: NIST SP 800-53A (v1): CP-4 (3).1

---

**CCI:** CCI-001603 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2010-05-12

**Definition:** The contingency plan identifies the primary storage site hazards.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-6 (1)
NIST: NIST SP 800-53A (v1): CP-6 (1).1 (i)

---

**CCI:** CCI-000506 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization initiates necessary alternate storage site agreements to permit the storage and recovery of information system backup information.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-6
NIST: NIST SP 800-53A (v1): CP-6.1 (ii)

---

**CCI:** CCI-001605 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2010-05-12

**Definition:** The contingency plan identifies the primary processing site hazards.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-7 (1)
NIST: NIST SP 800-53A (v1): CP-7 (1).1 (i)

---

**CCI:** CCI-000511 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization defines the time period for achieving the recovery time objectives for business functions within which processing must be resumed at the alternate processing site.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-7
NIST: NIST SP 800-53A (v1): CP-7.1 (ii)

---

**CCI:** CCI-000512 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization establishes an alternate processing site.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-7 a
NIST: NIST SP 800-53A (v1): CP-7.1 (i)

---

**CCI:** CCI-001607 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2010-05-12

**Definition:** The organization establishes alternate telecommunications services to support the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-8 (2)
NIST: NIST SP 800-53A (v1): CP-8.1 (i)

---

**CCI:** CCI-001608 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2010-05-12

**Definition:** The organization identifies the primary provider's telecommunications service hazards.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-8 (3)
NIST: NIST SP 800-53A (v1): CP-8 (3).1 (i)

---

**CCI:** CCI-000544 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization stores backup copies of the operating system in a separate facility or in a fire-rated container that is not colocated with the operational system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-9 (3)
NIST: NIST SP 800-53A (v1): CP-9 (3).1

---

**CCI:** CCI-000545 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization stores backup copies of critical information system software in a separate facility or in a fire-rated container that is not colocated with the operational system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-9 (3)
NIST: NIST SP 800-53A (v1): CP-9 (3).1

---

**CCI:** CCI-000546 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization stores backup copies of the information system inventory (including hardware, software, and firmware components) in a separate facility or in a fire-rated container that is not colocated with the operational system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): CP-9 (3)
NIST: NIST SP 800-53A (v1): CP-9 (3).1

---

**CCI:** CCI-000769 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-17

**Definition:** The organization allows the use of group authenticators only when used in conjunction with an individual/unique authenticator.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): IA-2 (5) (a)
NIST: NIST SP 800-53A (v1): IA-2 (5).1 (i)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000771 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |

**Definition:** The information system uses multifactor authentication for network access to privileged accounts where one of the factors is provided by a device separate from the information system being accessed.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): IA-2 (6)
NIST: NIST SP 800-53A (v1): IA-2 (6).1

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000772 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |

**Definition:** The information system uses multifactor authentication for network access to non-privileged accounts where one of the factors is provided by a device separate from the information system being accessed.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): IA-2 (7)
NIST: NIST SP 800-53A (v1): IA-2 (7).1

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000773 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |

**Definition:** The organization defines replay-resistant authentication mechanisms to be used for network access to privileged accounts.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): IA-2 (8)
NIST: NIST SP 800-53A (v1): IA-2 (8).1 (i)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000774 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |

**Definition:** The information system uses organization-defined replay-resistant authentication mechanisms for network access to privileged accounts.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): IA-2 (8)
NIST: NIST SP 800-53A (v1): IA-2 (8).1 (ii)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000775 | **Status:** | draft |

**Contributor:** DISA FSO **Published Date:** 2009-09-17

**Definition:** The organization defines replay-resistant authentication mechanisms to be used for network access to non-privileged accounts.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): IA-2 (9)
NIST: NIST SP 800-53A (v1): IA-2 (9).1 (i)

---

**CCI:** CCI-000776 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-17

**Definition:** The information system uses organization-defined replay-resistant authentication mechanisms for network access to non-privileged accounts.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): IA-2 (9)
NIST: NIST SP 800-53A (v1): IA-2 (9).1 (ii)

---

**CCI:** CCI-000779 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-17

**Definition:** The information system authenticates devices before establishing remote network connections using bidirectional authentication between devices that is cryptographically based.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): IA-3 (1)
NIST: NIST SP 800-53A (v1): IA-3 (1).1 (i)

---

**CCI:** CCI-000780 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-17

**Definition:** The information system authenticates devices before establishing wireless network connections using bidirectional authentication between devices that is cryptographically based.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): IA-3 (1)
NIST: NIST SP 800-53A (v1): IA-3 (1).1 (ii)

---

**CCI:** CCI-000781 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-17

**Definition:** The information system authenticates devices before establishing network connections using bidirectional authentication between devices that is cryptographically based.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): IA-3 (2)
NIST: NIST SP 800-53A (v1): IA-3 (2).1

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000782 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |
| **Definition:** | The organization standardizes, with regard to dynamic address allocation, Dynamic Host Control Protocol (DHCP) lease information and the time assigned to DHCP-enabled devices. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): IA-3 (3)<br>NIST: NIST SP 800-53A (v1): IA-3 (3).1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000784 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |
| **Definition:** | The organization manages information system identifiers for users and devices by receiving authorization from a designated organizational official to assign a user identifier. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): IA-4 a<br>NIST: NIST SP 800-53A (v1): IA-4.1 (iii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000785 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |
| **Definition:** | The organization manages information system identifiers for users and devices by receiving authorization from a designated organizational official to assign a device identifier. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): IA-4 a<br>NIST: NIST SP 800-53A (v1): IA-4.1 (iii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000786 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |
| **Definition:** | The organization manages information system identifiers for users and devices by selecting an identifier that uniquely identifies an individual. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): IA-4 b<br>NIST: NIST SP 800-53A (v1): IA-4.1 (iii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000787 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |
| **Definition:** | The organization manages information system identifiers for users and devices by selecting an identifier that uniquely identifies a device. | | |
| **Type:** | policy | | |

**References:** NIST: NIST SP 800-53 (v3): IA-4 b
NIST: NIST SP 800-53A (v1): IA-4.1 (iii)

---

**CCI:** CCI-000788 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-17
**Definition:** The organization manages information system identifiers for users and devices by assigning the user identifier to the intended party.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): IA-4 c
NIST: NIST SP 800-53A (v1): IA-4.1 (iii)

---

**CCI:** CCI-000789 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-17
**Definition:** The organization manages information system identifiers for users and devices by assigning the device identifier to the intended device.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): IA-4 c
NIST: NIST SP 800-53A (v1): IA-4.1 (iii)

---

**CCI:** CCI-000790 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-17
**Definition:** The organization defines a time period for which the reuse of user identifiers is prohibited.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): IA-4 d
NIST: NIST SP 800-53A (v1): IA-4.1 (i)

---

**CCI:** CCI-000791 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-17
**Definition:** The organization defines a time period for which the reuse of device identifiers is prohibited.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): IA-4 d
NIST: NIST SP 800-53A (v1): IA-4.1 (i)

---

**CCI:** CCI-000792 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-17
**Definition:** The organization manages information system identifiers for users and devices by preventing reuse of user identifiers for an organization-defined time period.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): IA-4 d

| | | | |
|---|---|---|---|
| | NIST: NIST SP 800-53A (v1): IA-4.1 (iii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000793 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |
| **Definition:** | The organization manages information system identifiers for users and devices by preventing reuse of device identifiers for an organization-defined time period. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): IA-4 d | | |
| | NIST: NIST SP 800-53A (v1): IA-4.1 (iii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000797 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |
| **Definition:** | The organization requires that registration to receive a user ID and password include authorization by a supervisor. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): IA-4 (2) | | |
| | NIST: NIST SP 800-53A (v1): IA-4 (2) (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000798 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |
| **Definition:** | The organization requires that registration to receive a user ID and password be done in person before a designated registration authority. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): IA-4 (2) | | |
| | NIST: NIST SP 800-53A (v1): IA-4 (2) (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000802 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-17 |
| **Definition:** | The information system dynamically manages identifiers, attributes, and associated access authorizations. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): IA-4 (5) | | |
| | NIST: NIST SP 800-53A (v1): IA-4 (5).1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001620 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-12 |
| **Definition:** | The organization defines the types of and/or specific authenticators for which the registration process must be carried out in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor). | | |
| **Type:** | policy | | |

**References:** NIST: NIST SP 800-53 (v3): IA-5 (3)
NIST: NIST SP 800-53A (v1): IA-5 (3).1 (i)

---

**CCI:** CCI-000175 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-05-22
**Definition:** The organization manages information system authenticators for users and devices by verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): IA-5 a
NIST: NIST SP 800-53A (v1): IA-5.1 (ii)

---

**CCI:** CCI-000177 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-05-22
**Definition:** The organization manages information system authenticators for users and devices by establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): IA-5 d
NIST: NIST SP 800-53A (v1): IA-5.1 (ii)

---

**CCI:** CCI-000178 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-05-22
**Definition:** The organization manages information system authenticators for users and devices by changing default content of authenticators upon information system installation.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): IA-5 e
NIST: NIST SP 800-53A (v1): IA-5.1 (ii)

---

**CCI:** CCI-000188 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-15
**Definition:** The organization requires that the registration process to receive an organizational-defined type of authenticator be carried out in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor).
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): IA-5 (3)
NIST: NIST SP 800-53A (v1): IA-5 (3).1 (ii)

---

**CCI:** CCI-000189 **Status:** draft
**Contributor:** DISA FSO **Published** 2009-09-15

| | | | |
|---|---|---|---|
| | | Date: | |
| **Definition:** | The organization employs automated tools to determine if authenticators are sufficiently strong to resist attacks intended to discover or otherwise compromise the authenticators. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): IA-5 (4)<br>NIST: NIST SP 800-53A (v1): IA-5 (4).1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000190 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-15 |
| **Definition:** | The organization requires vendors/manufacturers of information system components to provide unique authenticators or change default authenticators prior to delivery. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): IA-5 (5)<br>NIST: NIST SP 800-53A (v1): IA-5 (5).1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000191 | **Status:** | deprecated |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-15 |
| **Definition:** | The organization enforces password complexity by the number of special characters used. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): IA-5 (1) (a)<br>NIST: NIST SP 800-53A (v1): IA-5 (1).1 (v) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001622 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-12 |
| **Definition:** | The organization identifies personnel with incident response roles and responsibilities with respect to the information system. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): IR-2<br>NIST: NIST SP 800-53A (v1): IR-2.1 (i) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001623 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-12 |
| **Definition:** | The incident response training material addresses the procedures and activities necessary to fulfill identified organizational incident response roles and responsibilities. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): IR-2<br>NIST: NIST SP 800-53A (v1): IR-2.1 (iii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000843 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published** | 2009-09-18 |

**Date:**

**Definition:** The organization develops an incident response plan that provides the organization with a roadmap for implementing its incident response capability; describes the structure and organization of the incident response capability; provides a high-level approach for how the incident response capability fits into the overall organization; meets the unique requirements of the organization, which relate to mission, size, structure, and functions; defines reportable incidents; provides metrics for measuring the incident response capability within the organization; and defines the resources and management support needed to effectively maintain and mature an incident response capability.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): IR-8 a
NIST: NIST SP 800-53A (v1): IR-8.1

---

**CCI:** CCI-001629 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2010-05-12

**Definition:** The organization employs automated mechanisms to produce up-to-date, accurate, complete, and available records of all maintenance and repair actions needed, in process, and complete.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): MA-2 (2)
NIST: NIST SP 800-53A (v1): MA-2 (2).1 (ii)

---

**CCI:** CCI-000858 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): MA-2 a
NIST: NIST SP 800-53A (v1): MA-2.1 (i)

---

**CCI:** CCI-000863 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization maintains maintenance records for the information system that include the date and time of maintenance, the name of the individual performing the maintenance, the name of escort, if necessary, a description of the maintenance performed, and a list of equipment removed or replaced (including identification numbers, if applicable).

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): MA-2 (1) (a)(b)(c)(d)(e)
NIST: NIST SP 800-53A (v1): MA-2 (1).1

---

**CCI:** CCI-000864 **Status:** draft

**Contributor:** DISA FSO **Published** 2009-09-18

| | | | |
|---|---|---|---|
| | | **Date:** | |
| **Definition:** | The organization employs automated mechanisms to schedule, conduct, and document maintenance and repairs as required. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): MA-2 (2)<br>NIST: NIST SP 800-53A (v1): MA-2 (2).1(i) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000868 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |
| **Definition:** | The organization maintains, on an ongoing basis, information system maintenance tools. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): MA-3<br>NIST: NIST SP 800-53A (v1): MA-3.1 (ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000872 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |
| **Definition:** | The organization employs automated mechanisms to restrict the use of maintenance tools to authorized personnel only. | | |
| **Type:** | policy, technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): MA-3 (4)<br>NIST: NIST SP 800-53A (v1): MA-3 (4).1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001630 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-12 |
| **Definition:** | Designated organizational personnel review the maintenance records of the non-local maintenance and diagnostic sessions. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): MA-4 (1)<br>NIST: NIST SP 800-53A (v1): MA-4 (1).1 (ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000875 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |
| **Definition:** | The organization controls non-local maintenance and diagnostic activities. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): MA-4 a<br>NIST: NIST SP 800-53A (v1): MA-4.1 (i) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000880 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-18 |

**Definition:** The organization audits non-local maintenance and diagnostic sessions.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): MA-4 (1)
NIST: NIST SP 800-53A (v1): MA-4 (1).1 (i)

---

**CCI:** CCI-000885 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization requires that maintenance personnel notify organization-defined personnel when non-local maintenance is planned (i.e., date/time).

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): MA-4 (5) (a)
NIST: NIST SP 800-53A (v1): MA-4 (5).1 (ii)

---

**CCI:** CCI-000888 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization employs cryptographic mechanisms to protect the integrity and confidentiality of non-local maintenance and diagnostic communications.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): MA-4 (6)
NIST: NIST SP 800-53A (v1): MA-4 (6).1

---

**CCI:** CCI-000889 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization employs remote disconnect verification at the termination of non-local maintenance and diagnostic sessions.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): MA-4 (7)
NIST: NIST SP 800-53A (v1): MA-4 (7).1

---

**CCI:** CCI-000892 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization ensures that personnel performing maintenance on the information system have required access authorizations or designates organizational personnel with required access authorizations and technical competence deemed necessary to supervise information system maintenance.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): MA-5 b
NIST: NIST SP 800-53A (v1): MA-5.1 (iii)

---

**CCI:** CCI-000896 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization requires that in the event an information system component cannot be sanitized, the procedures contained in the security plan for the system be enforced.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): MA-5 (1) (c)
NIST: NIST SP 800-53A (v1): MA-5 (1).1

---

**CCI:** CCI-000901 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization defines a list of security-critical information system components and/or key information technology components for which it will obtain maintenance support and/or spare parts.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): MA-6
NIST: NIST SP 800-53A (v1): MA-6.1 (i)

---

**CCI:** CCI-000902 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-18

**Definition:** The organization defines a time period for obtaining maintenance support and/or spare parts for security-critical information system components and/or key information technology components.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): MA-6
NIST: NIST SP 800-53A (v1): MA-6.1 (ii)

---

**CCI:** CCI-001006 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization defines security measures for restricting access to media.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): MP-2
NIST: NIST SP 800-53A (v1): MP-2.1 (i)

---

**CCI:** CCI-001009 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The information system uses cryptographic mechanisms to protect and restrict access to information on portable digital media.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): MP-2 (2)
NIST: NIST SP 800-53A (v1): MP-2 (2).1

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001633 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-12 |
| **Definition:** | The organization defines removable media types and information output requiring marking. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): MP-3 a<br>NIST: NIST SP 800-53A (v1): MP-3.1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001017 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization defines security measures for securing media storage. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): MP-4 a<br>NIST: NIST SP 800-53A (v1): MP-4.1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001019 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization employs cryptographic mechanisms to protect information in storage. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): MP-4 (1)<br>NIST: NIST SP 800-53A (v1): MP-4 (1).1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001029 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization tracks, documents, and verifies media sanitization and disposal actions. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): MP-6 (1)<br>NIST: NIST SP 800-53A (v1): MP-6 (1).1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001034 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization sanitizes information system media containing Controlled Unclassified Information (CUI) or other sensitive information in accordance with applicable organizational and/or federal standards and policies. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): MP-6 (4)<br>NIST: NIST SP 800-53A (v1): MP-6 (4).1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001035 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published** | 2009-09-21 |

| | | | |
|---|---|---|---|
| | | **Date:** | |
| **Definition:** | The organization sanitizes information system media containing classified information in accordance with NSA standards and policies. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): MP-6 (5)<br>NIST: NIST SP 800-53A (v1): MP-6 (5).1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001036 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization destroys information system media that cannot be sanitized. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): MP-6 (6)<br>NIST: NIST SP 800-53A (v1): MP-6 (6).1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000960 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PE-11<br>NIST: NIST SP 800-53A (v1): PE-11.1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000962 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization provides a long-term alternate power supply for the information system that is self-contained and not reliant on external power generation. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PE-11 (2)<br>NIST: NIST SP 800-53A (v1): PE-11 (2).1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000964 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization provides emergency lighting for all areas within the facility supporting essential missions and business functions. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PE-12 (1)<br>NIST: NIST SP 800-53A (v1): PE-12 (1).1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000969 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published** | 2009-09-21 |

| | | | |
|---|---|---|---|
| | | **Date:** | |
| **Definition:** | The organization ensures that the facility undergoes, on an organization-defined frequency, fire marshal inspections and promptly resolves identified deficiencies. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PE-13 (4)<br>NIST: NIST SP 800-53A (v1): PE-13 (4).1 (ii and iii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000970 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization defines a frequency for fire marshal inspections. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PE-13 (4)<br>NIST: NIST SP 800-53A (v1): PE-13 (4).1 (i) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000966 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization employs fire detection devices/systems for the information system that activate automatically and notify the organization and emergency responders in the event of a fire. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PE-13 (1)<br>NIST: NIST SP 800-53A (v1): PE-13 (1).1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000967 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to the organization and emergency responders. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PE-13 (2)<br>NIST: NIST SP 800-53A (v1): PE-13 (2).1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000980 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization employs mechanisms that, without the need for manual intervention, protect the information system from water damage in the event of a water leak. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PE-15 (1)<br>NIST: NIST SP 800-53A (v1): PE-15 (1).1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000986 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization defines management, operational, and technical information system security controls to be employed at alternate work sites. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PE-17 a<br>NIST: NIST SP 800-53A (v1): PE-17.1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000990 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization positions information system components within the facility to minimize potential damage from environmental hazards. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PE-18<br>NIST: NIST SP 800-53A (v1): PE-18.1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000992 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization plans the location or site of the facility where the information system resides with regard to physical and environmental hazards, and for existing facilities, considers the physical and environmental hazards in its risk mitigation strategy. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PE-18 (1)<br>NIST: NIST SP 800-53A (v1): PE-18 (1).1 (i and ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001634 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-12 |
| **Definition:** | The organization identifies authorized personnel with appropriate clearances and access authorizations for gaining physical access to the facility containing an information system that processes classified information. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PE-2 (3)<br>NIST: NIST SP 800-53A (v1): PE-2 (3).1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000918 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization restricts physical access to the facility containing an information system that processes classified information to authorized personnel with appropriate clearances and access authorizations. | | |
| **Type:** | policy | | |

**References:** NIST: NIST SP 800-53 (v3): PE-2 (3)
NIST: NIST SP 800-53A (v1): PE-2 (3).1 (ii)

---

**CCI:** CCI-000922 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization controls access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): PE-3 d
NIST: NIST SP 800-53A (v1): PE-3.1 (iv)

---

**CCI:** CCI-000938 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization monitors physical access to the information system to detect and respond to physical security incidents.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): PE-6 a
NIST: NIST SP 800-53A (v1): PE-6.1 (i)

---

**CCI:** CCI-000943 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization employs automated mechanisms to recognize potential intrusions and initiate designated response actions.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): PE-6 (2)
NIST: NIST SP 800-53A (v1): PE-6 (2).1

---

**CCI:** CCI-000944 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): PE-7
NIST: NIST SP 800-53A (v1): PE-7.1

---

**CCI:** CCI-000945 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization escorts visitors and monitors visitor activity, when required.

| | | | |
|---|---|---|---|
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PE-7 (1)<br>NIST: NIST SP 800-53A (v1): PE-7 (1).1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000946 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization requires two forms of identification for visitor access to the facility. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PE-7 (2)<br>NIST: NIST SP 800-53A (v1): PE-7 (2).1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000951 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization maintains a record of all physical access, both visitor and authorized individuals. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PE-8 (2)<br>NIST: NIST SP 800-53A (v1): PE-8 (2).1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000953 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization employs redundant and parallel power cabling paths. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PE-9 (1)<br>NIST: NIST SP 800-53A (v1): PE-9 (1).1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000565 | **Status:** | deprecated |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization reviews/updates, per organization-defined frequency, a formal, documented security planning policy. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PL-1 a<br>NIST: NIST SP 800-53A (v1): PL-1.2 (ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000570 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization develops a security plan for the information system that is consistent with the organization's enterprise architecture; explicitly defines the authorization boundary for the system; describes the operational context of the information system in terms of mission | | |

and business processes; provides the security category and impact level of the information system, including supporting rationale; describes the operational environment for the information system; describes relationships with, or connections to, other information systems; provides an overview of the security requirements for the system; and describes the security controls in place or planned for meeting those requirements, including a rationale for the tailoring and supplemental decisions.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PL-2 a
NIST: NIST SP 800-53A (v1): PL-2.1 (i)

---

**CCI:** CCI-000576 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization develops a security Concept of Operations (CONOPS) for the information system containing, at a minimum: the purpose of the system; a description of the system architecture; the security authorization schedule; and the security categorization and associated factors considered in determining the categorization.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PL-2 (1) (a)
NIST: NIST SP 800-53A (v1): PL-2 (1).1 (i) (ii) (iii) (iv) (v)

---

**CCI:** CCI-000580 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization develops a functional architecture for the information system that identifies and maintains external interfaces.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PL-2 (2) (a)
NIST: NIST SP 800-53A (v1): PL-2 (2).1

---

**CCI:** CCI-000581 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization develops a functional architecture for the information system that identifies and maintains the information being exchanged across the interfaces.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PL-2 (2) (a)
NIST: NIST SP 800-53A (v1): PL-2 (2).1

---

**CCI:** CCI-000582 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization develops a functional architecture for the information system that identifies and maintains the protection mechanisms associated with each interface.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PL-2 (2) (a)
NIST: NIST SP 800-53A (v1): PL-2 (2).1

---

**CCI:** CCI-000583 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization develops a functional architecture for the information system that identifies and maintains user roles.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): PL-2 (2) (b)
NIST: NIST SP 800-53A (v1): PL-2 (2).1

---

**CCI:** CCI-000584 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization develops a functional architecture for the information system that identifies and maintains the access privileges assigned to each role.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): PL-2 (2) (b)
NIST: NIST SP 800-53A (v1): PL-2 (2).1

---

**CCI:** CCI-000585 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization develops a functional architecture for the information system that identifies and maintains unique security requirements.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): PL-2 (2) (c)
NIST: NIST SP 800-53A (v1): PL-2 (2).1

---

**CCI:** CCI-000586 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization develops a functional architecture for the information system that identifies and maintains types of information processed by the information system.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): PL-2 (2) (d)
NIST: NIST SP 800-53A (v1): PL-2 (2).1

---

**CCI:** CCI-000587 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21
**Definition:** The organization develops a functional architecture for the information system that identifies and maintains types of information stored by the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PL-2 (2) (d)
NIST: NIST SP 800-53A (v1): PL-2 (2).1

---

**CCI:** CCI-000588 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization develops a functional architecture for the information system that identifies and maintains types of information transmitted by the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PL-2 (2) (d)
NIST: NIST SP 800-53A (v1): PL-2 (2).1

---

**CCI:** CCI-000589 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization develops a functional architecture for the information system that identifies and maintains any specific protection needs in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PL-2 (2) (d)
NIST: NIST SP 800-53A (v1): PL-2 (2).1

---

**CCI:** CCI-000590 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization develops a functional architecture for the information system that identifies and maintains restoration priority of information.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PL-2 (2) (e)
NIST: NIST SP 800-53A (v1): PL-2 (2).1

---

**CCI:** CCI-000591 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization develops a functional architecture for the information system that identifies and maintains restoration priority of information system services.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PL-2 (2) (e)
NIST: NIST SP 800-53A (v1): PL-2 (2).1

---

**CCI:** CCI-000596 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization includes in the rules of behavior, explicit restrictions on sharing information system account information.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PL-4 (1)
NIST: NIST SP 800-53A (v1): PL-4 (1).1

---

**CCI:** CCI-000597 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization conducts a privacy impact assessment on the information system in accordance with OMB policy.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PL-5
NIST: NIST SP 800-53A (v1): PL-5.1 (i) (ii)

---

**CCI:** CCI-000598 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation).

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PL-6
NIST: NIST SP 800-53A (v1): PL-6.1

---

**CCI:** CCI-000599 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational assets.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PL-6
NIST: NIST SP 800-53A (v1): PL-6.1

---

**CCI:** CCI-000600 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational individuals.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): PL-6
NIST: NIST SP 800-53A (v1): PL-6.1

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000023 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-11-03 |
| **Definition:** | The organization develops an organization-wide information security program plan that provides sufficient information about the program management controls and common controls (including specification of parameters for any assignment and selection operations either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan, and a determination of the risk to be incurred if the plan is implemented as intended. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PM-1 a<br>NIST: NIST SP 800-53A (v1): PM-1.1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001543 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-11-03 |
| **Definition:** | The organization disseminates the most recent information security program plan to appropriate entities in the organization that includes roles, responsibilities, management commitment, coordination among organizational entities, and compliance. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PM-1 a<br>NIST: NIST SP 800-53A (v1): PM-1.1 (v) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001534 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-11-03 |
| **Definition:** | The organization ensures that access to information with special protection measures is granted only to individuals who have a valid access authorization that is demonstrated by assigned official government duties. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PS-6 (1) (a)<br>NIST: NIST SP 800-53A (v1): PS-6 (1).1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001535 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-11-03 |
| **Definition:** | The organization ensures that access to information with special protection measures is granted only to individuals who satisfy associated personnel security criteria. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): PS-6 (1) (b)<br>NIST: NIST SP 800-53A (v1): PS-6 (1).1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001644 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-12 |

**Definition:** The organization employs vulnerability scanning procedures that can demonstrate the depth of coverage (i.e., vulnerabilities checked).

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): RA-5 (3)
NIST: NIST SP 800-53A (v1): RA-5 (3).1 (ii)

---

**CCI:** CCI-001065 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization employs vulnerability scanning procedures that can demonstrate the breadth of coverage (i.e., information system components scanned).

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): RA-5 (3)
NIST: NIST SP 800-53A (v1): RA-5 (3).1 (i)

---

**CCI:** CCI-001069 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization employs automated mechanisms to detect the presence of unauthorized software on organizational information systems and notify designated organizational officials in accordance with the organization-defined frequency.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): RA-5 (7)
NIST: NIST SP 800-53A (v1): RA-5 (7).1 (ii)

---

**CCI:** CCI-001070 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization defines a frequency for employing automated mechanisms to detect the presence of unauthorized software on organizational information systems and notify designated organizational officials.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): RA-5 (7)
NIST: NIST SP 800-53A (v1): RA-5 (7).1 (i)

---

**CCI:** CCI-001072 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization employs an independent penetration agent or penetration team to conduct a vulnerability analysis on the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): RA-5 (9) (a)
NIST: NIST SP 800-53A (v1): RA-5 (9).1

---

**CCI:** CCI-001073 **Status:** draft

| | | | |
|---|---|---|---|
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization employs an independent penetration agent or penetration team to perform penetration testing on the information system based on the vulnerability analysis to determine the exploitability of identified vulnerabilities. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): RA-5 (9) (b)<br>NIST: NIST SP 800-53A (v1): RA-5 (9).1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001650 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-12 |
| **Definition:** | The organization requires the information system developers to manage and control changes to the information system during development. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SA-10 (b)<br>NIST: NIST SP 800-53A (v1): SA-10.1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001651 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-12 |
| **Definition:** | The organization requires the information system integrators to manage and control changes to the information system during development. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SA-10 (b)<br>NIST: NIST SP 800-53A (v1): SA-10.1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001652 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-12 |
| **Definition:** | The organization requires the information system developers to manage and control changes to the information system during implementation. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SA-10 (b)<br>NIST: NIST SP 800-53A (v1): SA-10.1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001653 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-12 |
| **Definition:** | The organization requires the information system integrators to manage and control changes to the information system during implementation. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SA-10 (b)<br>NIST: NIST SP 800-53A (v1): SA-10.1 (ii) | | |

**CCI:** CCI-001654 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2010-05-12
**Definition:** The organization requires the information system developers to manage and control changes to the information system during modification.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): SA-10 (b)
NIST: NIST SP 800-53A (v1): SA-10.1 (ii)

---

**CCI:** CCI-001655 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2010-05-12
**Definition:** The organization requires the information system integrators to manage and control changes to the information system during modification.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): SA-10 (b)
NIST: NIST SP 800-53A (v1): SA-10.1 (ii)

---

**CCI:** CCI-000682 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-22
**Definition:** The organization requires information system developers to perform configuration management during information system design.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): SA-10 (a)
NIST: NIST SP 800-53A (v1): SA-10.1 (i)

---

**CCI:** CCI-000683 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-22
**Definition:** The organization requires information system developers to perform configuration management during information system development.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): SA-10 (a)
NIST: NIST SP 800-53A (v1): SA-10.1 (i)

---

**CCI:** CCI-000684 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-22
**Definition:** The organization requires information system developers to perform configuration management during information system implementation.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): SA-10 (a)
NIST: NIST SP 800-53A (v1): SA-10.1 (i)

**CCI:** CCI-000685 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization requires information system developers to perform configuration management during information system operation.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-10 (a)

NIST: NIST SP 800-53A (v1): SA-10.1 (i)

---

**CCI:** CCI-000686 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization requires information system integrators to perform configuration management during information system design.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-10 (a)

NIST: NIST SP 800-53A (v1): SA-10.1 (i)

---

**CCI:** CCI-000687 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization requires information system integrators to perform configuration management during information system development.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-10 (a)

NIST: NIST SP 800-53A (v1): SA-10.1 (i)

---

**CCI:** CCI-000688 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization requires information system integrators to perform configuration management during information system implementation.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-10 (a)

NIST: NIST SP 800-53A (v1): SA-10.1 (i)

---

**CCI:** CCI-000689 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization requires information system integrators to perform configuration management during information system operation.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-10 (a)

NIST: NIST SP 800-53A (v1): SA-10.1 (i)

---

**CCI:** CCI-000690 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization requires information system developers to manage and control changes to the information system during design.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-10 (b)

NIST: NIST SP 800-53A (v1): SA-10.1 (ii)

---

**CCI:** CCI-000691 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization requires information system integrators to manage and control changes to the information system during design.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-10 (b)

NIST: NIST SP 800-53A (v1): SA-10.1 (ii)

---

**CCI:** CCI-000693 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization requires information system integrators to implement only organization-approved changes.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-10 (c)

NIST: NIST SP 800-53A (v1): SA-10.1 (iii)

---

**CCI:** CCI-000695 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization requires information system integrators to document approved changes to the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-10 (d)

NIST: NIST SP 800-53A (v1): SA-10.1 (iv)

---

**CCI:** CCI-000696 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization requires that information system developers track security flaws and flaw resolution.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-10 (e)

NIST: NIST SP 800-53A (v1): SA-10.1 (v)

---

**CCI:** CCI-000697 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization requires information system integrators to track security flaws and flaw resolution.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-10 (e)

NIST: NIST SP 800-53A (v1): SA-10.1 (v)

---

**CCI:** CCI-000699 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization requires information system integrators to provide an integrity check of software to facilitate organizational verification of software integrity after delivery.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-10 (1)

NIST: NIST SP 800-53A (v1): SA-10 (1).1

---

**CCI:** CCI-000701 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization provides an alternative configuration management process with organizational personnel in the absence of a dedicated integrator configuration management team.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-10 (2)

NIST: NIST SP 800-53A (v1): SA-10 (2).1

---

**CCI:** CCI-000702 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization requires information system developers, in consultation with associated security personnel (including security engineers), to create a security test and evaluation plan.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-11 (a)

NIST: NIST SP 800-53A (v1): SA-11.1 SA-11(3).1 (i)

---

**CCI:** CCI-000703 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization requires information system developers, in consultation with associated security personnel (including security engineers), to implement a security test and evaluation plan.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-11 (a)
NIST: NIST SP 800-53A (v1): SA-11.1

---

**CCI:** CCI-000704 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization requires information system integrators, in consultation with associated security personnel (including security engineers), to create a security test and evaluation plan.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-11 (a)
NIST: NIST SP 800-53A (v1): SA-11.1 SA-11(3).1 (i)

---

**CCI:** CCI-000705 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization requires information system integrators, in consultation with associated security personnel (including security engineers), to implement a security test and evaluation plan.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-11 (a)
NIST: NIST SP 800-53A (v1): SA-11.1

---

**CCI:** CCI-000706 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization requires information system developers, in consultation with associated security personnel (including security engineers), to implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-11 (b)
NIST: NIST SP 800-53A (v1): SA-11.1

---

**CCI:** CCI-000707 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization requires information system integrators, in consultation with associated security personnel (including security engineers), to implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-11 (b)

NIST: NIST SP 800-53A (v1): SA-11.1

---

**CCI:** CCI-000708 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization requires information system developers, in consultation with associated security personnel (including security engineers), to document the results of the security testing/evaluation processes.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-11 (c)

NIST: NIST SP 800-53A (v1): SA-11.1

---

**CCI:** CCI-000709 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization requires information system developers, in consultation with associated security personnel (including security engineers), to document the results of the security flaw remediation processes.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-11 (c)

NIST: NIST SP 800-53A (v1): SA-11.1

---

**CCI:** CCI-000710 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization requires information system integrators, in consultation with associated security personnel (including security engineers), to document the results of the security testing/evaluation processes.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-11 (c)

NIST: NIST SP 800-53A (v1): SA-11.1

---

**CCI:** CCI-000711 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization requires information system integrators, in consultation with associated security personnel (including security engineers), to document the results of the security flaw remediation processes.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-11 (c)

NIST: NIST SP 800-53A (v1): SA-11.1

---

**CCI:** CCI-000712 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization requires information system developers to employ code analysis tools to examine software for common flaws and document the results of the analysis.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-11 (1)

NIST: NIST SP 800-53A (v1): SA-11 (1).1 (i) (ii)

---

**CCI:** CCI-000713 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization requires information system integrators to employ code analysis tools to examine software for common flaws and document the results of the analysis.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-11 (1)

NIST: NIST SP 800-53A (v1): SA-11 (1).1 (i) (ii)

---

**CCI:** CCI-000714 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization requires information system developers to perform a vulnerability analysis to document vulnerabilities.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-11 (2)

NIST: NIST SP 800-53A (v1): SA-11 (*2).1

---

**CCI:** CCI-000715 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization requires information system developers to perform a vulnerability analysis to document exploitation potential.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-11 (2)

NIST: NIST SP 800-53A (v1): SA-11 (2).1

---

**CCI:** CCI-000716 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization requires information system developers to perform a vulnerability analysis to document risk mitigations.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-11 (2)

NIST: NIST SP 800-53A (v1): SA-11 (2).1

---

**CCI:** CCI-000717 **Status:** draft

**Contributor:** DISA FSO **Published** 2009-09-22

| | | | |
|---|---|---|---|
| | | **Date:** | |
| **Definition:** | The organization requires information system integrators to perform a vulnerability analysis to document vulnerabilities. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SA-11 (2)<br>NIST: NIST SP 800-53A (v1): SA-11 (2).1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000718 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization requires information system integrators to perform a vulnerability analysis to document exploitation potential. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SA-11 (2)<br>NIST: NIST SP 800-53A (v1): SA-11 (2).1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000719 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization requires information system integrators perform a vulnerability analysis to document risk mitigations. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SA-11 (2)<br>NIST: NIST SP 800-53A (v1): SA-11 (2).1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000720 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization requires information system developers implement the security test and evaluation plan under the witness of an independent verification and validation agent. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SA-11 (3)<br>NIST: NIST SP 800-53A (v1): SA-1 1(3).1 (ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000721 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization requires information system integrators to implement the security test and evaluation plan under the witness of an independent verification and validation agent. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SA-11 (3)<br>NIST: NIST SP 800-53A (v1): SA-1 1(3).1 (ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000724 | **Status:** | draft |

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization purchases all anticipated information system components and spares in the initial acquisition.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-12 (1)
NIST: NIST SP 800-53A (v1): SA-12 (1).1

---

**CCI:** CCI-000725 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization conducts a due diligence review of suppliers prior to entering into contractual agreements to acquire information system hardware.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-12 (2)
NIST: NIST SP 800-53A (v1): SA-12 (2).1

---

**CCI:** CCI-000726 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization conducts a due diligence review of suppliers prior to entering into contractual agreements to acquire information system software.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-12 (2)
NIST: NIST SP 800-53A (v1): SA-12 (2).1

---

**CCI:** CCI-000727 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization conducts a due diligence review of suppliers prior to entering into contractual agreements to acquire information system firmware.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-12 (2)
NIST: NIST SP 800-53A (v1): SA-12 (2).1

---

**CCI:** CCI-000728 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization conducts a due diligence review of suppliers prior to entering into contractual agreements to acquire information system services.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-12 (2)
NIST: NIST SP 800-53A (v1): SA-12 (2).1

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000729 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization uses trusted shipping for information systems. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SA-12 (3)<br>NIST: NIST SP 800-53A (v1): SA-12 (3).1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000730 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization uses trusted shipping for information system components. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SA-12 (3)<br>NIST: NIST SP 800-53A (v1): SA-12 (3).1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000731 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization uses trusted shipping for information technology products. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SA-12 (3)<br>NIST: NIST SP 800-53A (v1): SA-12 (3).1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000732 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization uses trusted warehousing for information systems. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SA-12 (3)<br>NIST: NIST SP 800-53A (v1): SA-12 (3).1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000733 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization uses trusted warehousing for information system components. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SA-12 (3)<br>NIST: NIST SP 800-53A (v1): SA-12 (3).1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000734 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization uses trusted warehousing for information technology products. | | |

**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): SA-12 (3)
NIST: NIST SP 800-53A (v1): SA-12 (3).1

---

**CCI:** CCI-000735 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-22
**Definition:** The organization employs a diverse set of suppliers for information systems.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): SA-12 (4)
NIST: NIST SP 800-53A (v1): SA-12 (4).1

---

**CCI:** CCI-000736 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-22
**Definition:** The organization employs a diverse set of suppliers for information system components.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): SA-12 (4)
NIST: NIST SP 800-53A (v1): SA-12 (4).1

---

**CCI:** CCI-000737 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-22
**Definition:** The organization employs a diverse set of suppliers for information technology products.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): SA-12 (4)
NIST: NIST SP 800-53A (v1): SA-12 (4).1

---

**CCI:** CCI-000738 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-22
**Definition:** The organization employs a diverse set of suppliers for information system services.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): SA-12 (4)
NIST: NIST SP 800-53A (v1): SA-12 (4).1

---

**CCI:** CCI-000739 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-22
**Definition:** The organization employs standard configurations for information systems.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): SA-12 (5)
NIST: NIST SP 800-53A (v1): SA-12 (5).1

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000740 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization employs standard configurations for information system components. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SA-12 (5)<br>NIST: NIST SP 800-53A (v1): SA-12 (5).1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000741 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization employs standard configurations for information technology products. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SA-12 (5)<br>NIST: NIST SP 800-53A (v1): SA-12 (5).1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000742 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization minimizes the time between purchase decisions and delivery of information systems. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SA-12 (6)<br>NIST: NIST SP 800-53A (v1): SA-12 (6).1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000743 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization minimizes the time between purchase decisions and delivery of information system components. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SA-12 (6)<br>NIST: NIST SP 800-53A (v1): SA-12 (6).1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000744 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization minimizes the time between purchase decisions and delivery of information technology products. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SA-12 (6)<br>NIST: NIST SP 800-53A (v1): SA-12 (6).1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000745 | **Status:** | draft |

| | | | |
|---|---|---|---|
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization employs independent analysis and penetration testing against delivered information systems. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SA-12 (7) | | |
| | NIST: NIST SP 800-53A (v1): SA-12 (7).1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000746 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization employs independent analysis and penetration testing against delivered information system components. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SA-12 (7) | | |
| | NIST: NIST SP 800-53A (v1): SA-12 (7).1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000747 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization employs independent analysis and penetration testing against delivered information technology products. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SA-12 (7) | | |
| | NIST: NIST SP 800-53A (v1): SA-12 (7).1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000748 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization defines level of trustworthiness for the information system. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SA-13 | | |
| | NIST: NIST SP 800-53A (v1): SA-13.1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000749 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization requires that the information system meets the organization-defined level of trustworthiness. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SA-13 | | |
| | NIST: NIST SP 800-53A (v1): SA-13.1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000750 | **Status:** | draft |

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization defines the list of critical information system components that require re-implementation.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-14

NIST: NIST SP 800-53A (v1): SA-14.1 (i)

---

**CCI:** CCI-000751 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization determines the organization-defined list of critical information system components that require re-implementation.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-14 a

NIST: NIST SP 800-53A (v1): SA-14

---

**CCI:** CCI-000752 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization re-implements organization-defined critical information system components.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-14 b

NIST: NIST SP 800-53A (v1): SA-14.1 (ii)

---

**CCI:** CCI-000753 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization identifies information system components for which alternative sourcing is not viable.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-14 (1) (a)

NIST: NIST SP 800-53A (v1): SA-14 (1).1 (i)

---

**CCI:** CCI-000754 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization defines measures to be employed to prevent critical security controls for information system components from being compromised.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-14 (1) (b)

NIST: NIST SP 800-53A (v1): SA-14 (1).1 (ii)

---

**CCI:** CCI-000755 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization employs organization-defined measures to ensure critical security controls for the information system components are not compromised.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-14 (1) (b)

NIST: NIST SP 800-53A (v1): SA-14 (1).1 (iii)

---

**CCI:** CCI-000608 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization includes a determination of information security requirements for the information system in mission process planning.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-2 a

NIST: NIST SP 800-53A (v1): SA-2.1 (i)

---

**CCI:** CCI-000609 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization includes a determination of information security requirements for the information system in business process planning.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-2 a

NIST: NIST SP 800-53A (v1): SA-2.1 (i)

---

**CCI:** CCI-000617 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization documents information system security roles and responsibilities throughout the system development life cycle.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-3 b

NIST: NIST SP 800-53A (v1): SA-3.1 (ii)

---

**CCI:** CCI-001647 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2010-05-12

**Definition:** The organization requires the use of a FIPS-validated, cryptographic module for a technology product that relies on cryptographic functionality to enforce its security policy when no U.S. Government Protection Profile exists for such a specific technology type.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-4 (7) (b)

NIST: NIST SP 800-53A (v1): SA-4 (7).1 (iii)

---

**CCI:** CCI-000619 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization includes security functional requirements/specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-4 a

NIST: NIST SP 800-53A (v1): SA-4.1

---

**CCI:** CCI-000620 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization includes security-related documentation requirements, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-4 b

NIST: NIST SP 800-53A (v1): SA-4.1

---

**CCI:** CCI-000621 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization includes developmental and evaluation-related assurance requirements, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-4 c

NIST: NIST SP 800-53A (v1): SA-4.1

---

**CCI:** CCI-000624 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization requires in acquisition documents that vendors/contractors provide information describing the design details of the security controls to be employed within the information system, information system components, or information system services (including functional interfaces among control components) in sufficient detail to permit analysis and testing of the controls.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-4 (2)

NIST: NIST SP 800-53A (v1): SA-4 (2).1

---

**CCI:** CCI-000625

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2009-09-21

**Definition:** The organization requires in acquisition documents that vendors/contractors provide information describing the implementation details of the security controls to be employed within the information system, information system components, or information system services (including functional interfaces among control components) in sufficient detail to permit analysis and testing of the controls.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-4 (2)
NIST: NIST SP 800-53A (v1): SA-4 (2).1

---

**CCI:** CCI-000626

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2009-09-21

**Definition:** The organization requires software vendors/manufacturers to minimize flawed or malformed software by demonstrating that their software development process employs state-of-the-practice software and security engineering methods.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-4 (3)
NIST: NIST SP 800-53A (v1): SA-4 (3).1

---

**CCI:** CCI-000627

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2009-09-21

**Definition:** The organization requires software vendors/manufacturers to minimize flawed or malformed software by demonstrating that their software development process employs quality control processes.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-4 (3)
NIST: NIST SP 800-53A (v1): SA-4 (3).1

---

**CCI:** CCI-000628

**Status:** draft

**Contributor:** DISA FSO

**Published Date:** 2009-09-21

**Definition:** The organization requires software vendors/manufacturers to minimize flawed or malformed software by demonstrating that their software development processes employ validation techniques.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-4 (3)
NIST: NIST SP 800-53A (v1): SA-4 (3).1

---

**CCI:** CCI-000629

**Status:** draft

**Contributor:** DISA FSO

**Published** 2009-09-21

**Date:**

**Definition:** The organization ensures each information system component acquired is explicitly assigned to an information system, and that the owner of the system acknowledges this assignment.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-4 (4)
NIST: NIST SP 800-53A (v1): SA-4 (4).1 (i) (ii)

---

**CCI:** CCI-000630 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization requires in acquisition documents, that information system components are delivered in a secure, documented configuration, and that the secure configuration is the default configuration for any software reinstalls or upgrades.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-4 (5)
NIST: NIST SP 800-53A (v1): SA-4 (5).1 (i) (ii)

---

**CCI:** CCI-000632 **Status:** deprecated

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization employs only commercial off-the-shelf (COTS) information assurance (IA) and IA-enabled information technology products that compose an NSA-approved solution to protect classified information when the networks used to transmit the information are at a lower classification level than the information being transmitted.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-4 (6) (a)
NIST: NIST SP 800-53A (v1): SA-4 (6).1 (i)

---

**CCI:** CCI-001648 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2010-05-12

**Definition:** The organization makes available to authorized personnel the source code for the information system to permit analysis and testing.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-5 (5)
NIST: NIST SP 800-53A (v1): SA-5 (5).1

---

**CCI:** CCI-000636 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization obtains administrator documentation for the information system that describes secure configuration, installation, and operation of the information system; effective use and maintenance of the security features/functions; and known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-5 a<br>
NIST: NIST SP 800-53A (v1): SA-5.1 (i)

---

**CCI:** CCI-000637 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization protects, as required, administrator documentation for the information system that describes secure configuration, installation, and operation of the information system; effective use and maintenance of the security features/functions; and known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-5 a<br>
NIST: NIST SP 800-53A (v1): SA-5.1 (i)

---

**CCI:** CCI-000638 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization makes available to authorized personnel administrator documentation for the information system that describes secure configuration, installation, and operation of the information system; effective use and maintenance of the security features/functions; and known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-5 a<br>
NIST: NIST SP 800-53A (v1): SA-5.1 (i)

---

**CCI:** CCI-000639 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization obtains user documentation for the information system that describes user-accessible security features/functions and how to effectively use those security features/functions; methods for user interaction with the information system, which enables individuals to use the system in a more secure manner; and user responsibilities in maintaining the security of the information and information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-5 b<br>
NIST: NIST SP 800-53A (v1): SA-5.1 (ii)

---

**CCI:** CCI-000640 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization protects, as required, user documentation for the information system that describes user-accessible security features/functions and how to effectively use those security features/functions; methods for user interaction with the information system, which enables individuals to use the system in a more secure manner; and user responsibilities in maintaining the security of the information and information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-5 b<br>NIST: NIST SP 800-53A (v1): SA-5.1 (ii)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000641 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |

**Definition:** The organization makes available to authorized personnel user documentation for the information system that describes user-accessible security features/functions and how to effectively use those security features/functions; methods for user interaction with the information system, which enables individuals to use the system in a more secure manner; and user responsibilities in maintaining the security of the information and information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-5 b<br>NIST: NIST SP 800-53A (v1): SA-5.1 (ii)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000643 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |

**Definition:** The organization obtains vendor/manufacturer documentation that describes the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-5 (1)<br>NIST: NIST SP 800-53A (v1): SA-5 (1).1 (i) SA-5(2).1 (i)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000644 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |

**Definition:** The organization protects, as required, vendor/manufacturer documentation that describes the functional properties of the security controls employed within the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-5 (1)<br>NIST: NIST SP 800-53A (v1): SA-5 (1).1 (i) SA-5(2).1 (i)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000645 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |

**Definition:** The organization makes available to authorized personnel vendor/manufacturer documentation that describes the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-5 (2)

| | | | |
|---|---|---|---|
| | NIST: NIST SP 800-53A (v1): SA-5 (1).1 SA-5(2).1 SA-5(3).1 SA-5(4).1 (i)s | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000646 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization obtains vendor/manufacturer documentation that describes the security-relevant external interfaces to the information system with sufficient detail to permit analysis and testing. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SA-5 (2)<br>NIST: NIST SP 800-53A (v1): SA-5 (1).1 SA-5(2).1 SA-5(3).1 SA-5(4) (ii)s | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000647 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization obtains vendor/manufacturer documentation that describes the high-level design of the information system in terms of subsystems and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SA-5 (3)<br>NIST: NIST SP 800-53A (v1): SA-5 (3).1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000648 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization protects, as required, vendor/manufacturer documentation that describes the high-level design of the information system in terms of subsystems and implementation details of the security controls employed within the system. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SA-5 (3)<br>NIST: NIST SP 800-53A (v1): SA-5 (3).1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000650 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization obtains vendor/manufacturer documentation that describes the low-level design of the information system in terms of modules and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SA-5 (4)<br>NIST: NIST SP 800-53A (v1): SA-5 (4).1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000651 | **Status:** | draft |

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization protects, as required, vendor/manufacturer documentation that describes the low-level design of the information system in terms of modules and implementation details of the security controls employed within the system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-5 (4)
NIST: NIST SP 800-53A (v1): SA-5 (4).1 (ii)

---

**CCI:** CCI-000653 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization obtains the source code for the information system to permit analysis and testing.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-5 (5)
NIST: NIST SP 800-53A (v1): SA-5 (5).1

---

**CCI:** CCI-000654 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization protects, as required, the source code for the information system to permit analysis and testing.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-5 (5)
NIST: NIST SP 800-53A (v1): SA-5 (5).1

---

**CCI:** CCI-001690 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2011-10-07

**Definition:** The organization protects, as required, vendor/manufacturer documentation that describes the security-relevant external interfaces to the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-5 (1)
NIST: NIST SP 800-53A (v1): SA-5 (1).1 (i)

---

**CCI:** CCI-001691 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2011-10-07

**Definition:** The organization makes available to authorized personnel vendor/manufacturer documentation that describes the security-relevant external interfaces to the information system with sufficient detail to permit analysis and testing.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-5 (1)
NIST: NIST SP 800-53A (v1): SA-5 (1).1 (i)

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001692 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2011-10-07 |
| **Definition:** | The organization makes available to authorized personnel vendor/manufacturer documentation that describes the low-level design of the information system in terms of modules and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SA-5 (4)<br>NIST: NIST SP 800-53A (v1): SA-5 (4).1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000655 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization uses software and associated documentation in accordance with contract agreements and copyright laws. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SA-6 a<br>NIST: NIST SP 800-53A (v1): SA-6.1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000656 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization employs tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SA-6 b<br>NIST: NIST SP 800-53A (v1): SA-6.1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000657 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization controls the use of peer-to-peer file sharing technology to ensure this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SA-6 c<br>NIST: NIST SP 800-53A (v1): SA-6.1 (iii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000658 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization documents the use of peer-to-peer file sharing technology to ensure this capability is not used for the unauthorized distribution, display, performance, or | | |

| | | | |
|---|---|---|---|
| | reproduction of copyrighted work. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SA-6 c<br>NIST: NIST SP 800-53A (v1): SA-6.1 (iii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000659 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization prohibits the use of binary executable code from sources with limited or no warranty without accompanying source code. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SA-6 (1) (a)<br>NIST: NIST SP 800-53A (v1): SA-6 (1).1 (i) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000660 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization prohibits the use of machine executable code from sources with limited or no warranty without accompanying source code. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SA-6 (1) (a)<br>NIST: NIST SP 800-53A (v1): SA-6 (1).1 (i) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000661 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization provides exceptions to the source code requirement only when no alternative solutions are available to support compelling mission/operational requirements. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SA-6 (1) (b)<br>NIST: NIST SP 800-53A (v1): SA-6 (1).1 (ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-000662 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization obtains express written consent of the authorizing official for exceptions to the source code requirement. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SA-6 (1) (b)<br>NIST: NIST SP 800-53A (v1): SA-6 (1).1 (iii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001649 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-12 |

**Definition:** The organization identifies and documents (as appropriate) explicit rules to be enforced when governing the installation of software by users.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-7
NIST: NIST SP 800-53A (v1): SA-7.1 (i)

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-000663 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |

**Definition:** The organization (or information system) enforces explicit rules governing the installation of software by users.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SA-7
NIST: NIST SP 800-53A (v1): SA-7.1 (ii)

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-000675 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |

**Definition:** The organization monitors security control compliance by external service providers.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-9 c
NIST: NIST SP 800-53A (v1): SA-9.1 (iii)

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-000676 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |

**Definition:** The organization conducts an organizational assessment of risk prior to the acquisition of dedicated information security services.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-9 (1) (a)
NIST: NIST SP 800-53A (v1): SA-9 (1).1 (i)

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-000677 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |

**Definition:** The organization conducts an organizational assessment of risk prior to the outsourcing of dedicated information security services.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-9 (1) (a)
NIST: NIST SP 800-53A (v1): SA-9 (1).1 (i)

---

|  |  |  |  |
|---|---|---|---|
| **CCI:** | CCI-000678 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |

**Definition:** The organization defines the senior organizational official designated to approve acquisition of dedicated information security services.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-9 (1) (b)
NIST: NIST SP 800-53A (v1): SA-9 (1).1 (ii)

---

**CCI:** CCI-000679 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization defines the senior organizational official designated to approve outsourcing of dedicated information security services.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-9 (1) (b)
NIST: NIST SP 800-53A (v1): SA-9 (1).1 (ii)

---

**CCI:** CCI-000680 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization ensures the acquisition of dedicated information security services is approved by an organization-designated senior organizational official.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-9 (1) (b)
NIST: NIST SP 800-53A (v1): SA-9 (1).1 (iii)

---

**CCI:** CCI-000681 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization ensures the outsourcing of dedicated information security services is approved by an organization-designated senior organizational official.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SA-9 (1) (b)
NIST: NIST SP 800-53A (v1): SA-9 (1).1 (iii)

---

**CCI:** CCI-001136 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization defines security functions include information system authentication and reauthentication.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-11
NIST: NIST SP 800-53A (v1): SC-11.1 (ii)

---

**CCI:** CCI-001137 **Status:** draft

**Contributor:** DISA FSO **Published** 2009-09-21

| | | | |
|---|---|---|---|
| | | Date: | |
| Definition: | The organization establishes cryptographic keys for required cryptography employed within the information system. | | |
| Type: | policy | | |
| References: | NIST: NIST SP 800-53 (v3): SC-12<br>NIST: NIST SP 800-53A (v1): SC-12.1 | | |

| | | | |
|---|---|---|---|
| CCI: | CCI-001138 | Status: | draft |
| Contributor: | DISA FSO | Published Date: | 2009-09-21 |
| Definition: | The organization manages cryptographic keys for required cryptography employed within the information system. | | |
| Type: | policy | | |
| References: | NIST: NIST SP 800-53 (v3): SC-12<br>NIST: NIST SP 800-53A (v1): SC-12.1 | | |

| | | | |
|---|---|---|---|
| CCI: | CCI-001140 | Status: | draft |
| Contributor: | DISA FSO | Published Date: | 2009-09-21 |
| Definition: | The organization produces, controls, and distributes symmetric cryptographic keys using NIST-approved or NSA-approved key management technology and processes. | | |
| Type: | technical | | |
| References: | NIST: NIST SP 800-53 (v3): SC-12 (2)<br>NIST: NIST SP 800-53A (v1): SC-12 (2).1 | | |

| | | | |
|---|---|---|---|
| CCI: | CCI-001141 | Status: | draft |
| Contributor: | DISA FSO | Published Date: | 2009-09-21 |
| Definition: | The organization produces, controls, and distributes symmetric and asymmetric cryptographic keys using NSA-approved key management technology and processes. | | |
| Type: | technical | | |
| References: | NIST: NIST SP 800-53 (v3): SC-12 (3)<br>NIST: NIST SP 800-53A (v1): SC-12 (3).1 | | |

| | | | |
|---|---|---|---|
| CCI: | CCI-001142 | Status: | draft |
| Contributor: | DISA FSO | Published Date: | 2009-09-21 |
| Definition: | The organization produces, controls, and distributes asymmetric cryptographic keys using approved PKI Class 3 certificates or prepositioned keying material. | | |
| Type: | technical | | |
| References: | NIST: NIST SP 800-53 (v3): SC-12 (4)<br>NIST: NIST SP 800-53A (v1): SC-12 (4).1 | | |

| | | | |
|---|---|---|---|
| CCI: | CCI-001143 | Status: | draft |

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization produces, controls, and distributes asymmetric cryptographic keys using approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user's private key.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SC-12 (5)
NIST: NIST SP 800-53A (v1): SC-12 (5).1

---

**CCI:** CCI-001144 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The information system implements required cryptographic protections using cryptographic modules that comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SC-13
NIST: NIST SP 800-53A (v1): SC-13.1

---

**CCI:** CCI-001145 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization employs, at a minimum, FIPS-validated cryptography to protect unclassified information.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SC-13 (1)
NIST: NIST SP 800-53A (v1): SC-13 (1).1

---

**CCI:** CCI-001146 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization employs NSA-approved cryptography to protect classified information.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SC-13 (2)
NIST: NIST SP 800-53A (v1): SC013 (2(.1

---

**CCI:** CCI-001147 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization employs, at a minimum, FIPS-validated cryptography to protect information when such information must be separated from individuals who have the necessary clearances yet lack the necessary access approvals.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SC-13 (3)
NIST: NIST SP 800-53A (v1): SC-13 (3).1

**CCI:** CCI-001149 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The information system protects the integrity and availability of publicly available information and applications.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SC-14
NIST: NIST SP 800-53A (v1): SC-14.1

---

**CCI:** CCI-001154 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The information system or supporting environment blocks both inbound and outbound traffic between instant messaging clients that are independently configured by end users and external service providers.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SC-15 (2)
NIST: NIST SP 800-53A (v1): SC-15 (2).1

---

**CCI:** CCI-001180 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The information system performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources when requested by client systems.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SC-21
NIST: NIST SP 800-53A (v1): SC-21.1

---

**CCI:** CCI-001181 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The information system performs data origin authentication and data integrity verification on all resolution responses received whether or not local client systems explicitly request this service.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SC-21 (1)
NIST: NIST SP 800-53A (v1): SC-21 (1).1

---

**CCI:** CCI-001186 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The information system provides a readily observable logout capability whenever authentication is used to gain access to web pages.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SC-23 (2)
NIST: NIST SP 800-53A (v1): SC-23 (2).1

---

**CCI:** CCI-001187 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The information system generates a unique session identifier for each session.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SC-23 (3)
NIST: NIST SP 800-53A (v1): SC-23 (3).1 (i)

---

**CCI:** CCI-001666 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2010-05-12

**Definition:** The organization employs cryptographic mechanisms to prevent unauthorized modification of information at rest unless otherwise protected by alternative physical measures.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-28 (1)
NIST: NIST SP 800-53A (v1): SC-28 (1).1 (ii)

---

**CCI:** CCI-001200 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information at rest unless otherwise protected by alternative physical measures.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SC-28 (1)
NIST: NIST SP 800-53A (v1): SC-28 (1).1 (i)

---

**CCI:** CCI-001656 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2010-05-12

**Definition:** The organization defines the security functions of the information system to be isolated from nonsecurity functions.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-3
NIST: NIST SP 800-53A (v1): SC-3.1 (i)

---

**CCI:** CCI-001087 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization implements an information system isolation boundary to minimize the number of nonsecurity functions included within the boundary containing security functions.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SC-3 (3)
NIST: NIST SP 800-53A (v1): SC-3 (3).1

---

**CCI:** CCI-001088 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization implements security functions as largely independent modules that avoid unnecessary interactions between modules.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-3 (4)
NIST: NIST SP 800-53A (v1): SC-3 (4).1

---

**CCI:** CCI-001202 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization employs virtualization techniques to present information system components as other types of components, or components with differing configurations.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-30
NIST: NIST SP 800-53A (v1): SC-30.1

---

**CCI:** CCI-001205 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization employs randomness in the implementation of the virtualization techniques.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-30 (2)
NIST: NIST SP 800-53A (v1): SC-30 (2).1

---

**CCI:** CCI-001206 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization requires that information system developers/integrators perform a covert channel analysis to identify those aspects of system communication that are potential avenues for covert storage and timing channels.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-31
NIST: NIST SP 800-53A (v1): SC-31.1

---

**CCI:** CCI-001208 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21

| | | | |
|---|---|---|---|
| **Definition:** | The organization partitions the information system into components residing in separate physical domains (or environments) as deemed necessary. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SC-32<br>NIST: NIST SP 800-53A (v1): SC-32.1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001209 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The information system protects the integrity of information during the processes of data aggregation, packaging, and transformation in preparation for transmission. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): SC-33<br>NIST: NIST SP 800-53A (v1): SC-33.1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001091 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The information system does not share resources that are used to interface with systems operating at different security levels. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): SC-4 (1)<br>NIST: NIST SP 800-53A (v1): SC-4 (1).1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001092 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The information system protects against or limits the effects of the organization-defined or referenced types of denial of service attacks. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): SC-5<br>NIST: NIST SP 800-53A (v1): SC-5.1 (ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001096 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The information system limits the use of resources by priority. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): SC-6<br>NIST: NIST SP 800-53A (v1): SC-6.1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001657 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-12 |

**Definition:** The organization defines the external boundary of the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-7 a
NIST: NIST SP 800-53A (v1): SC-7.1 (i)

---

**CCI:** CCI-001658 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2010-05-12

**Definition:** The organization defines key internal boundaries of the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-7 a
NIST: NIST SP 800-53A (v1): SC-7.1 (ii)

---

**CCI:** CCI-001659 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2010-05-12

**Definition:** The organization defines the mediation necessary for public access to the organization's internal networks.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-7 (2)
NIST: NIST SP 800-53A (v1): SC-7 (2).1 (i)

---

**CCI:** CCI-001660 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2010-05-12

**Definition:** The organization defines the measures to protect against unauthorized physical connections across boundary protections implemented at organization-defined managed interfaces.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-7 (14)
NIST: NIST SP 800-53A (v1): SC-7 (14).1 (ii)

---

**CCI:** CCI-001099 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization physically allocates publicly accessible information system components to separate subnetworks with separate physical network interfaces.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SC-7 (1)
NIST: NIST SP 800-53A (v1): SC-7 (1).1

---

**CCI:** CCI-001100 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-21

| | | | |
|---|---|---|---|
| **Definition:** | The information system prevents public access into the organization's internal networks except as appropriately mediated by managed interfaces employing boundary protection devices. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): SC-7 (2)<br>NIST: NIST SP 800-53A (v1): SC-7 (2).1 (ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001104 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization employs security controls as needed to protect the confidentiality and integrity of the information being transmitted. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SC-7 (4) (c)<br>NIST: NIST SP 800-53A (v1): SC-7 (4).1 (iv) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001110 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization prevents the unauthorized release of information outside of the information system boundary or any unauthorized communication through the information system boundary when there is an operational failure of the boundary protection mechanisms. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SC-7 (6)<br>NIST: NIST SP 800-53A (v1): SC-7 (6).1 (i) (ii) | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001111 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The information system prevents remote devices that have established a non-remote connection with the system from communicating outside of that communications path with resources in external networks. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): SC-7 (7)<br>NIST: NIST SP 800-53A (v1): SC-7 (7).1 | | |

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001115 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The information system, at managed interfaces, denies network traffic and audits internal users (or malicious code) posing a threat to external information systems. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): SC-7 (9)<br>NIST: NIST SP 800-53A (v1): SC-7 (9).1 (i) (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001117 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The information system checks incoming communications to ensure the communications are coming from an authorized source and routed to an authorized destination. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): SC-7 (11)<br>NIST: NIST SP 800-53A (v1): SC-7 (11).1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001118 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The information system implements host-based boundary protection mechanisms for servers, workstations, and mobile devices. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): SC-7 (12)<br>NIST: NIST SP 800-53A (v1): SC-7 (12).1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001127 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The information system protects the integrity of transmitted information. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): SC-8<br>NIST: NIST SP 800-53A (v1): SC-8.1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001128 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The organization employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): SC-8 (1)<br>NIST: NIST SP 800-53A (v1): SC-8 (1).1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001129 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-21 |
| **Definition:** | The information system maintains the integrity of information during aggregation, packaging, and transformation in preparation for transmission. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): SC-8 (2)<br>NIST: NIST SP 800-53A (v1): SC-8 (2).1 | | |

**CCI:** CCI-001130 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The information system protects the confidentiality of transmitted information.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SC-9

NIST: NIST SP 800-53A (v1): SC-9.1

---

**CCI:** CCI-001131 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SC-9 (1)

NIST: NIST SP 800-53A (v1): SC-9 (1).1

---

**CCI:** CCI-001132 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-21

**Definition:** The information system maintains the confidentiality of information during aggregation, packaging, and transformation in preparation for transmission.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SC-9 (2)

NIST: NIST SP 800-53A (v1): SC-9 (2).1

---

**CCI:** CCI-001311 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The information system identifies potentially security-relevant error conditions.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SI-11 a

NIST: NIST SP 800-53A (v1): SI-11.1 (i)

---

**CCI:** CCI-001313 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization defines sensitive or potentially harmful information that should not be contained in error logs and administrative messages.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SI-11 b

NIST: NIST SP 800-53A (v1): SI-11.1 (ii)

---

**CCI:** CCI-001679 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2010-05-12
**Definition:** The organization provides a mechanism to exchange active and standby roles of the components.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): SI-13 b
NIST: NIST SP 800-53A (v1): SI-13.1 (iv)

---

**CCI:** CCI-001316 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-22
**Definition:** The organization protects the information system from harm by considering mean time to failure rates for an organization-defined list of information system components in specific environments of operation.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): SI-13 a
NIST: NIST SP 800-53A (v1): SI-13.1 (ii)

---

**CCI:** CCI-001317 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-22
**Definition:** The organization defines a list of information system components for which mean time to failure rates should be considered to protect the information system from harm.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): SI-13 a
NIST: NIST SP 800-53A (v1): SI-13.1 (i)

---

**CCI:** CCI-001689 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2011-05-27
**Definition:** The organization, if an information system component failure is detected, automatically shuts down the information system.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): SI-13 (4) (b)
NIST: NIST SP 800-53A (v1): SI-13 (4).1 (iii)

---

**CCI:** CCI-001667 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2010-05-12
**Definition:** The organization compares the time measured between flaw identification and flaw remediation with organization-defined benchmarks.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): SI-2 (3)

NIST: NIST SP 800-53A (v1): SI-2 (3).1 (iii)

---

**CCI:** CCI-001232 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-22
**Definition:** The organization installs software updates automatically.
**Type:** technical
**References:** NIST: NIST SP 800-53 (v3): SI-2 (1)
NIST: NIST SP 800-53A (v1): SI-2 (1).1

---

**CCI:** CCI-001237 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-22
**Definition:** The organization employs automated patch management tools to facilitate flaw remediation to organization-defined information system components.
**Type:** technical
**References:** NIST: NIST SP 800-53 (v3): SI-2 (4)
NIST: NIST SP 800-53A (v1): SI-2 (4).1 (ii)

---

**CCI:** CCI-001238 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-22
**Definition:** The organization defines information system components for which automated patch management tools are to be employed to facilitate flaw remediation.
**Type:** policy
**References:** NIST: NIST SP 800-53 (v3): SI-2 (4)
NIST: NIST SP 800-53A (v1): SI-2 (4).1 (i)

---

**CCI:** CCI-001668 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2010-05-12
**Definition:** The organization employs malicious code protection mechanisms at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means or inserted through the exploitation of information system vulnerabilities.
**Type:** technical
**References:** NIST: NIST SP 800-53 (v3): SI-3 a
NIST: NIST SP 800-53A (v1): SI-3.1 (ii)

---

**CCI:** CCI-001239 **Status:** draft
**Contributor:** DISA FSO **Published Date:** 2009-09-22
**Definition:** The organization employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code transported by electronic mail,

electronic mail attachments, web accesses, removable media, or other common means or inserted through the exploitation of information system vulnerabilities.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SI-3 a<br>
NIST: NIST SP 800-53A (v1): SI-3.1 (i)

---

**CCI:** CCI-001248 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The information system prevents non-privileged users from circumventing malicious code protection capabilities.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SI-3 (3)<br>
NIST: NIST SP 800-53A (v1): SI-3 (3).1

---

**CCI:** CCI-001250 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization does not allow users to introduce removable media into the information system.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SI-3 (5)<br>
NIST: NIST SP 800-53A (v1): SI-3 (5).1

---

**CCI:** CCI-001672 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2010-05-12

**Definition:** The organization employs a wireless intrusion detection system to identify rogue wireless devices.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SI-4 (14)<br>
NIST: NIST SP 800-53A (v1): SI-4 (14).1 (ii)

---

**CCI:** CCI-001252 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization monitors events on the information system in accordance with organization-defined monitoring objectives and detects information system attacks.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SI-4 a<br>
NIST: NIST SP 800-53A (v1): SI-4.1 (ii)

---

**CCI:** CCI-001254 **Status:** draft

**Contributor:** DISA FSO **Published** 2009-09-22

**Date:**

**Definition:** The organization identifies unauthorized use of the information system.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SI-4 b
NIST: NIST SP 800-53A (v1): SI-4.1 (iii)

---

**CCI:** CCI-001259 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization interconnects and configures individual intrusion detection tools into a systemwide intrusion detection system using common protocols.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SI-4 (1)
NIST: NIST SP 800-53A (v1): SI-4 (1).1

---

**CCI:** CCI-001261 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SI-4 (3)
NIST: NIST SP 800-53A (v1): SI-4 (3).1

---

**CCI:** CCI-001262 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SI-4 (4)
NIST: NIST SP 800-53A (v1): SI-4

---

**CCI:** CCI-001263 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The information system provides near real-time alerts when any of the organization-defined list of compromise or potential compromise indicators occurs.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SI-4 (5)
NIST: NIST SP 800-53A (v1): SI-4 (5).1 (ii)

---

**CCI:** CCI-001265 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The information system prevents non-privileged users from circumventing intrusion detection and prevention capabilities.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SI-4 (6)
NIST: NIST SP 800-53A (v1): SI-4 (6).1

---

**CCI:** CCI-001269 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization protects information obtained from intrusion monitoring tools from unauthorized access, modification, and deletion.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SI-4 (8)
NIST: NIST SP 800-53A (v1): SI-4 (8).1

---

**CCI:** CCI-001272 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization makes provisions so encrypted traffic is visible to information system monitoring tools.

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SI-4 (10)
NIST: NIST SP 800-53A (v1): SI-4 (10).1

---

**CCI:** CCI-001278 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization uses the traffic/event profiles in tuning system monitoring devices to reduce the number of false positives to an organization-defined measure of false positives and the number of false negatives to an organization-defined measure of false negatives.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SI-4 (13) (c)
NIST: NIST SP 800-53A (v1): SI-4 (13).1 (iv)

---

**CCI:** CCI-001279 **Status:** draft

**Contributor:** DISA FSO **Published Date:** 2009-09-22

**Definition:** The organization defines the respective measurements to which the organization must tune system monitoring devices to reduce the number of false positives.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SI-4 (13) (c)
NIST: NIST SP 800-53A (v1): SI-4 (13).1 (iii)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001280 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization defines the respective measurements to which the organization must tune system monitoring devices to reduce the number of false negatives. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SI-4 (13) (c)<br>NIST: NIST SP 800-53A (v1): SI-4 (13).1 (iii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001281 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization employs a wireless intrusion detection system. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SI-4 (14)<br>NIST: NIST SP 800-53A (v1): SI-4 (14).1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001674 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-12 |
| **Definition:** | The information system responds to security function anomalies in accordance with organization-defined responses and alternative action(s). | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): SI-6<br>NIST: NIST SP 800-53A (v1): SI-6.1 (v) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001676 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-12 |
| **Definition:** | The organization defines, for periodic security function verification, the frequency of the verifications. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SI-6<br>NIST: NIST SP 800-53A (v1): SI-6.1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001291 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The information system verifies the correct operation of security functions in accordance with organization-defined conditions and in accordance with organization-defined frequency (if periodic verification). | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): SI-6<br>NIST: NIST SP 800-53A (v1): SI-6.1 (iv) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001292 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization defines the appropriate conditions, including the system transitional states if applicable, for verifying the correct operation of security functions. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SI-6<br>NIST: NIST SP 800-53A (v1): SI-6.1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001293 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization defines the information system responses and alternative action(s) to anomalies discovered during security function verification. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SI-6<br>NIST: NIST SP 800-53A (v1): SI-6.1 (iii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001297 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The information system detects unauthorized changes to software and information. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): SI-7<br>NIST: NIST SP 800-53A (v1): SI-7.1 | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001298 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization reassesses the integrity of software and information by performing, on an organization-defined frequency, integrity scans of the information system. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SI-7 (1)<br>NIST: NIST SP 800-53A (v1): SI-7 (1).1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001299 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization defines the frequency of integrity scans to be performed on the information system. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SI-7 (1)<br>NIST: NIST SP 800-53A (v1): SI-7 (1).1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001302 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization requires use of tamper-evident packaging for organization-defined information system components during organization-defined conditions. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SI-7 (4)<br>NIST: NIST SP 800-53A (v1): SI-7 (4).1 (iii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001303 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization defines information system components that require tamper-evident packaging. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SI-7 (4)<br>NIST: NIST SP 800-53A (v1): SI-7 (4).1 (i) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001304 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization defines conditions (i.e., transportation from vendor to operational site, during operation, both) under which tamper-evident packaging must be used for organization-defined information system components. | | |
| **Type:** | policy | | |
| **References:** | NIST: NIST SP 800-53 (v3): SI-7 (4)<br>NIST: NIST SP 800-53A (v1): SI-7 (4).1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001677 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2010-05-12 |
| **Definition:** | The organization employs spam protection mechanisms at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means. | | |
| **Type:** | technical | | |
| **References:** | NIST: NIST SP 800-53 (v3): SI-8 a<br>NIST: NIST SP 800-53A (v1): SI-8.1 (ii) | | |

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001305 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |
| **Definition:** | The organization employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means. | | |

**Type:** technical

**References:** NIST: NIST SP 800-53 (v3): SI-8 a<br>
NIST: NIST SP 800-53A (v1): SI-8.1 (i)

---

| | | | |
|---|---|---|---|
| **CCI:** | CCI-001309 | **Status:** | draft |
| **Contributor:** | DISA FSO | **Published Date:** | 2009-09-22 |

**Definition:** The organization restricts the capability to input information to the information system to authorized personnel.

**Type:** policy

**References:** NIST: NIST SP 800-53 (v3): SI-9<br>
NIST: NIST SP 800-53A (v1): SI-9.1

---