Control Correlation Identifier (CCI)

Confidentiality: Low; **Integrity:** Low; **Availability:** Low

Control Number	800-53 Control Text Indicator	CCI	CCI Definition	Implementation Guidance	Assessment Procedures
AC-1	AC-1 (a)	CCI-002107	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.	DoD has defined the personnel or roles as all personnel.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as all personnel.
AC-1	AC-1 (a)	CCI-002108	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.	DoD has defined the personnel or roles as all personnel.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as all personnel.
AC-1	AC-1 (a) (1)	CCI-000001	The organization develops and documents an access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	The organization being inspected/assessed develops and documents an access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	The organization conducting the inspection/assessment obtains and examines the access control policy to ensure the organization being inspected/assessed develops and documents an access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
AC-1	AC-1 (a) (1)	CCI-000002	The organization disseminates the access control policy to organization-defined personnel or roles.	The organization being inspected/assessed disseminates via an information sharing capability to all personnel. DoD has defined the personnel or roles as all personnel.	The organization conducting the inspection/assessment examines the access control policy via the organization's information sharing capability to ensure the organization being inspected/assessed disseminates the policy to all personnel. DoD has defined the personnel or roles as all personnel.
AC-1	AC-1 (a) (2)	CCI-000004	The organization develops and documents procedures to facilitate the implementation of the access control policy and associated access controls.	The organization being inspected/assessed develops and documents procedures to facilitate the implementation of the access control policy and associated access controls.	The organization conducting the inspection/assessment obtains and examines the procedures to facilitate the implementation of the access control policy and associated access controls to ensure the organization being inspected/assessed develops and documents procedures to facilitate the implementation of the access control policy and associated access controls.
AC-1	AC-1 (a) (2)	CCI-000005	The organization disseminates the procedures to facilitate access control policy and associated access controls to the organization-defined personnel or roles .	The organization being inspected/assessed disseminates via an information sharing capability to all personnel the procedures to facilitate access control policy and associated access controls. DoD has defined the personnel or roles as all personnel.	The organization conducting the inspection/assessment examines the procedures to facilitate access control policy and associated access controls via the organization's information sharing capability to ensure the organization being inspected/assessed disseminates the procedures to all personnel. DoD has defined the personnel or roles as all personnel.
AC-1	AC-1 (b) (1)	CCI-001545	The organization defines a frequency for reviewing and updating the access control policy.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.
AC-1	AC-1 (b) (1)	CCI-000003	The organization reviews and updates the access control policy in accordance with organization-defined frequency.	The organization being inspected/assessed annually reviews and updates the access control policy. The organization must maintain review and update activity as an audit trail. DoD has defined the frequency as annually.	The organization conducting the inspection/assessment obtains and examines the audit trail of reviews and updates to ensure the organization being inspected/assessed annually reviews and updates the access control policy. DoD has defined the frequency as annually.
AC-1	AC-1 (b) (2)	CCI-001546	The organization defines a frequency for reviewing and updating the access control procedures.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.
AC-1	AC-1 (b) (2)	CCI-000006	The organization reviews and updates the access control procedures in accordance with organization-defined frequency.	The organization being inspected/assessed annually reviews and updates the access control procedures. The organization must maintain review and update activity as an audit trail. DoD has defined the frequency as annually.	The organization conducting the inspection/assessment obtains and examines the audit trail of reviews and updates to ensure the organization being inspected/assessed annually reviews and updates the access control procedures. DoD has defined the frequency as annually.

AC-2	AC-2 (a)	CCI-002110	The organization defines the information system account types that support the organizational missions/business functions.	The organization being inspected/assessed defines and documents the information system account types that support the organizational missions/business functions. DoD has determined the information system account types are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented information system account types to ensure the organization being inspected/assessed defines the information system account types that support the organizational missions/business functions. DoD has determined the information system account types are not appropriate to define at the Enterprise level.
AC-2	AC-2 (a)	CCI-002111	The organization identifies and selects the organization-defined information system account types of information system accounts which support organizational missions/business functions.	The account types are defined per AC-2, CCI 2110.	The account types are defined per AC-2, CCI 2110.
AC-2	AC-2 (b)	CCI-002112	The organization assigns account managers for information system accounts.	The organization being inspected/assessed documents personnel responsible for the management of system accounts.	The organization conducting the inspection/assessment obtains and examines the documented appointment of management personnel to ensure that the organization being inspected/assessed has documented personnel responsible for the management of system accounts.
AC-2	AC-2 (c)	CCI-000008	The organization establishes conditions for group membership.	The organization being inspected/assessed documents conditions for adding accounts as members of groups.	The organization conducting the inspection/assessment obtains and examines the documented conditions for adding accounts as members of groups to ensure that the conditions are established.
AC-2	AC-2 (c)	CCI-002113	The organization establishes conditions for role membership.	The organization being inspected/assessed documents conditions for adding accounts as members of roles.	The organization conducting the inspection/assessment obtains and examines the documented conditions for adding accounts as members of roles to ensure that the conditions are established.
AC-2	AC-2 (d)	CCI-002115	The organization specifies authorized users of the information system.	The organization being inspected/assessed documents authorized users of the information system.	The organization conducting the inspection/assessment obtains and examines the documented list of authorized users for a sampling of information system accounts to ensure that the authorized users are specified.
AC-2	AC-2 (d)	CCI-002116	The organization specifies authorized group membership on the information system.	The organization being inspected/assessed documents authorized group membership on the information system.	The organization conducting the inspection/assessment obtains and examines the documented list of authorized groups for a sampling of information system accounts to ensure that the authorized groups are specified.
AC-2	AC-2 (d)	CCI-002117	The organization specifies authorized role membership on the information system.	The organization being inspected/assessed documents authorized role membership on the information system.	The organization conducting the inspection/assessment obtains and examines the documented list of authorized roles for a sampling of information system accounts to ensure that the authorized roles are specified
AC-2	AC-2 (d)	CCI-002118	The organization specifies access authorizations (i.e., privileges) for each account on the information system.	The organization being inspected/assessed documents access authorizations (i.e., privileges) for each account on the information system.	The organization conducting the inspection/assessment obtains and examines the documented list of access authorizations for a sampling of information system accounts to ensure that the access authorizations are specified.
AC-2	AC-2 (d)	CCI-002119	The organization specifies other attributes for each account on the information system.	The organization being inspected/assessed documents other attributes for each account on the information system.	The organization conducting the inspection/assessment obtains and examines the documented list of other attributes for a sampling of information system accounts to ensure that other attributes are specified.
AC-2	AC-2 (e)	CCI-002120	The organization defines the personnel or roles authorized to approve the creation of information system accounts.	DoD has defined the personnel or roles as the ISSM or ISSO.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as the ISSM or ISSO.
AC-2	AC-2 (e)	CCI-000010	The organization requires approvals by organization-defined personnel or roles for requests to create information system accounts.	The organization being inspected/assessed implements a process for the ISSM or ISSO to approve information system account requests. The organization being inspected/assessed maintains an audit trail of approvals. DoD has defined the personnel or roles as the ISSM or ISSO.	The organization conducting the inspection/assessment obtains and examines the audit trail of approvals to ensure that the organization being inspected/assessed implements a process for the ISSM or ISSO to approve information system account requests. DoD has defined the personnel or roles as the ISSM or ISSO.
AC-2	AC-2 (f)	CCI-002121	The organization defines the procedures or conditions to be employed when creating, enabling, modifying, disabling, and removing information system accounts.	The organization being inspected/assessed defines and documents the procedures or conditions to be employed when creating, enabling, modifying, disabling, and removing information system accounts. DoD has determined the procedures or conditions are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented procedures or conditions to ensure the organization being inspected/assessed defines the procedures or conditions to be employed when creating, enabling, modifying, disabling, and removing information system accounts. DoD has determined the procedures or conditions are not appropriate to define at the Enterprise level.

AC-2	AC-2 (f)	CCI-000011	The organization creates, enables, modifies, disables, and removes information system accounts in accordance with organization-defined procedures or conditions.	The organization being inspected/assessed implements account maintenance processes to create, enable, modify, disable, and remove information system accounts in accordance with procedures or conditions defined in AC-2, 2121. The organization being inspected/assessed maintains an audit trail of account maintenance activities.	The organization conducting the inspection/assessment obtains and examines the audit trail of account maintenance activities to ensure the organization being inspected/assessed implements account maintenance processes to create, enable, modify, disable, remove, and track information system accounts in accordance with procedures or conditions defined in AC-2, 2121.
AC-2	AC-2 (g)	CCI-002122	The organization monitors the use of information system accounts.	The organization being inspected/assessed implements a process to monitor the use of information system accounts.	The organization conducting the inspection/assessment obtains and examines the audit trail to ensure that the organization being inspected/assessed implements a process to monitor the use of information system accounts.
AC-2	AC-2 (h) (1)	CCI-002123	The organization notifies account managers when accounts are no longer required.	The organization being inspected/assessed implements a process to notify account managers when accounts are no longer required. The organization being inspected/assessed maintains an audit trail of notifications.	The organization conducting the inspection/assessment obtains and examines the audit trail of notifications to ensure the organization being inspected/assessed implements a process to notify account managers when accounts are no longer required.
AC-2	AC-2 (h) (2)	CCI-002124	The organization notifies account managers when users are terminated or transferred.	The organization being inspected/assessed implements a process to notify account managers when users are terminated or transferred. The organization being inspected/assessed maintains an audit trail of notifications.	The organization conducting the inspection/assessment obtains and examines the audit trail of notifications to ensure the organization being inspected/assessed implements a process to notify account managers when users are terminated or transferred.
AC-2	AC-2 (h) (3)	CCI-002125	The organization notifies account managers when individual information system usage or need-to-know changes.	The organization being inspected/assessed implements a process to notify account managers when individual information system usage or need-to-know changes. The organization being inspected/assessed maintains an audit trail of notifications.	The organization conducting the inspection/assessment obtains and examines the audit trail of notifications to ensure the organization being inspected/assessed implements a process to notify account managers when individual information system usage or need-to-know changes.
AC-2	AC-2 (i) (1)	CCI-002126	The organization authorizes access to the information system based on a valid access authorization.	The organization being inspected/assessed authorizes access to the information system based on the access authorization process. The organization being inspected/assessed maintains an audit trail of approved access.	The organization conducting the inspection/assessment obtains and examines the audit trail of approved access to ensure the organization being inspected/assessed authorizes access to the information system based on the access authorization process.
AC-2	AC-2 (i) (2)	CCI-002127	The organization authorizes access to the information system based on intended system usage.	The organization being inspected/assessed authorizes access to the information system based on intended system usage. The organization being inspected/assessed maintains an audit trail of approved access.	The organization conducting the inspection/assessment obtains and examines the audit trail of approved access to ensure the organization being inspected/assessed authorizes access to the information system based on intended system usage.
AC-2	AC-2 (i) (3)	CCI-002128	The organization authorizes access to the information system based on other attributes as required by the organization or associated missions/business functions.	The organization being inspected/assessed authorizes access to the information system based on other attributes as required by the organization or associated missions/business functions. The organization being inspected/assessed maintains an audit trail of approved access.	The organization conducting the inspection/assessment obtains and examines the audit trail of approved access to ensure the organization being inspected/assessed authorizes access to the information system based on other attributes as required by the organization or associated missions/business functions.
AC-2	AC-2 (j)	CCI-000012	The organization reviews information system accounts for compliance with account management requirements per organization-defined frequency.	The organization being inspected/assessed implements a process to review information system accounts for compliance with account management requirements at a minimum, annually. The organization being inspected/assessed maintains an audit trail of reviews. DoD has defined the frequency as at a minimum, annually.	The organization conducting the inspection/assessment obtains and examines the audit trail of reviews to ensure the organizaiton being inspected/assessed implements a process to review information system accounts for compliance with account management requirements at a minimum, annually. DoD has defined the frequency as at a minimum, annually.
AC-2	AC-2 (j)	CCI-001547	The organization defines the frequency on which it will review information system accounts for compliance with account management requirements.	DoD has defined the frequency as at a minimum, annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as at a minimum, annually.

AC-2	AC-2 (k)	CCI-002129	The organization establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.	The organization being inspected/assessed includes in the account management procedures a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.	The organization conducting the inspection/assessment obtains and examines the account management procedures to ensure the organization being inspected/assessed includes in the account management procedures a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.
AC-2 (4)	AC-2 (4)	CCI-000018	The information system automatically audits account creation actions.	The organization being inspected/assessed configures the information system to automatically audit account creation actions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 18.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to automatically audit account creation actions. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 18.
AC-2 (4)	AC-2 (4)	CCI-001403	The information system automatically audits account modification actions.	The organization being inspected/assessed configures the information system to automatically audit account modification actions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1403.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to automatically audit account modification actions. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1403.
AC-2 (4)	AC-2 (4)	CCI-002130	The information system automatically audits account enabling actions.	The organization being inspected/assessed configures the information system to automatically audit account enabling actions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2130.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to automatically audit account enabling actions. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2130.
AC-2 (4)	AC-2 (4)	CCI-001404	The information system automatically audits account disabling actions.	The organization being inspected/assessed configures the information system to automatically audit account disabling actions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1404.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to automatically audit account disabling actions. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1404.
AC-2 (4)	AC-2 (4)	CCI-001405	The information system automatically audits account removal actions.	The organization being inspected/assessed configures the information system to automatically audit account removal actions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1405.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to automatically audit account removal actions. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1405.

AC-2 (4)	AC-2 (4)	CCI-001683	The information system notifies organization-defined personnel or roles for account creation actions.	The organization being inspected/assessed configures the information system to notify the system administrator and ISSO for account creation actions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1683. DoD has defined the personnel or roles as the system administrator and ISSO.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to notify the system administrator and ISSO for account creation actions. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1683. DoD has defined the personnel or roles as the system administrator and ISSO.
AC-2 (4)	AC-2 (4)	CCI-001684	The information system notifies organization-defined personnel or roles for account modification actions.	The organization being inspected/assessed configures the information system to notify the system administrator and ISSO for account modification actions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1684. DoD has defined the personnel or roles as the system administrator and ISSO.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to notify the system administrator and ISSO for account modification actions. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1684. DoD has defined the personnel or roles as the system administrator and ISSO.
AC-2 (4)	AC-2 (4)	CCI-002132	The information system notifies organization-defined personnel or roles for account enabling actions.	The organization being inspected/assessed configures the information system to notify the system administrator and ISSO for account enabling actions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2132. DoD has defined the personnel or roles as the system administrator and ISSO.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to notify the system administrator and ISSO for account enabling actions. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2132. DoD has defined the personnel or roles as the system administrator and ISSO.
AC-2 (4)	AC-2 (4)	CCI-001685	The information system notifies organization-defined personnel or roles for account disabling actions.	The organization being inspected/assessed configures the information system to notify the system administrator and ISSO for account disabling actions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1685. DoD has defined the personnel or roles as the system administrator and ISSO.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to notify the system administrator and ISSO for account disabling actions. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1685. DoD has defined the personnel or roles as the system administrator and ISSO.
AC-2 (4)	AC-2 (4)	CCI-001686	The information system notifies organization-defined personnel or roles for account removal actions.	The organization being inspected/assessed configures the information system to notify the system administrator and ISSO for account removal actions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1686. DoD has defined the personnel or roles as the system administrator and ISSO.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to notify the system administrator and ISSO for account removal actions. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1686. DoD has defined the personnel or roles as the system administrator and ISSO.

AC-2 (4)	AC-2 (4)	CCI-002131	The organization defines the personnel or roles to be notified on account creation, modification, enabling, disabling, and removal actions.	DoD has defined the personnel or roles as the system administrator and ISSO.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as the system administrator and ISSO.
AC-2 (5)	AC-2 (5)	CCI-002133	The organization defines other conditions when users are required to log out.	The organization being inspected/assessed defines and documents the other conditions when users are required to log out. DoD has determined the conditions are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented conditions to ensure they have been defined. DoD has determined the conditions are not appropriate to define at the Enterprise level.
AC-2 (5)	AC-2 (5) (a)	CCI-000019	The organization requires that users log out in accordance with the organization-defined time period of inactivity and/or description of when to log out.	The organization being inspected/assessed documents in the user policies that users are required to log out at the end of the users standard work period unless otherwise defined in formal organizational policy and IAW conditions defined in AC-2 (5) CCI 2133. DoD has defined the time period as at the end of the users standard work period unless otherwise defined in formal organizational policy.	The organization conducting the inspection/assessment obtains and examines the user policies to ensure that users are required to log out at the end of the users standard work period unless otherwise defined in formal organizational policy and IAW conditions defined in AC-2 (5) CCI 2133. DoD has defined the time period as at the end of the users standard work period unless otherwise defined in formal organizational policy.
AC-2 (5)	AC-2 (5) (a)	CCI-001406	The organization defines a time period of expected inactivity when users are required to log out.	DoD has defined the time period as at the end of the users standard work period unless otherwise defined in formal organizational policy.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as at the end of the users standard work period unless otherwise defined in formal organizational policy.
AC-2 (7)	AC-2 (7) (a)	CCI-001358	The organization establishes privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles.	The organization being inspected/assessed documents and implements a process to establish privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles.	The organization conducting the inspection/assessment obtains and examines documented processes for privileged user account creation to ensure the organization being inspected/assessed establishes privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles.
AC-2 (7)	AC-2 (7) (a)	CCI-001407	The organization administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles.	The organization being inspected/assessed documents and implements a process to administer privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles.	The organization conducting the inspection/assessment obtains and examines documented processes for privileged user account creation to ensure the organization being inspected/assessed administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles.
AC-2 (7)	AC-2 (7) (b)	CCI-001360	The organization monitors privileged role assignments.	The organization being inspected/assessed implements a process to monitor privileged role assignments. The organization must maintain an audit trail of monitoring.	The organization conducting the inspection/assessment obtains and examines the audit trail of monitoring to ensure the organization being inspected/assessed monitors privileged role assignments.
AC-2 (7)	AC-2 (7) (c)	CCI-002136	The organization defines the actions to be taken when privileged role assignments are no longer appropriate	DoD has defined the actions as disables (or revokes) privileged user account.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the actions as disables (or revokes) privileged user account.
AC-2 (7)	AC-2 (7) (c)	CCI-002137	The organization takes organization-defined actions when privileged role assignments are no longer appropriate.	The organization being inspected/assessed documents and implements a process to disable (or revoke) the privileged user account when privileged role assignments are no longer appropriate. The organization must maintain an audit trail of the actions taken. DoD has defined the actions as disables (or revokes) privileged user account.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of actions taken to ensure the organization being inspected/assessed disables (or revokes) the privileged user accoun when privileged role assignments are no longer appropriate. DoD has defined the actions as disables (or revokes) privileged user account.
AC-2 (9)	AC-2 (9)	CCI-002140	The organization defines the conditions for establishing shared/group accounts.	The organization being inspected/assessed defines and documents the conditions for establishing shared/group accounts. DoD has determined the conditions are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented conditions to ensure they have been defined. DoD has determined the conditions are not appropriate to define at the Enterprise level.
AC-2 (9)	AC-2 (9)	CCI-002141	The organization only permits the use of shared/group accounts that meet organization-defined conditions for establishing shared/group accounts.	The organization being inspected/assessed only permits the use of shared/group accounts that meet the conditions for establishing shared/group accounts defined in AC-2 (9), CCI 2140.	The organization conducting the inspection/assessment examines the shared/group accounts to ensure the organization being inspected/assessed only permits the use of shared/group accounts that meet the conditions for establishing shared/group accounts defined in AC-2 (9), CCI 2140.

AC-2 (10)	AC-2 (10)	CCI-002142	The information system terminates shared/group account credentials when members leave the group.	The organization being inspected/assessed configures the information system to terminate shared/group account credentials when members leave the group. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2142.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to terminate shared/group account credentials when members leave the group. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2142.
AC-2 (12)	AC-2 (12) (a)	CCI-002146	The organization defines atypical usage for which the information system accounts are to be monitored.	The organization being inspected/assessed defines and documents atypical usage for which the information system accounts are to be monitored. DoD has determined atypical usage is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented atypical usage to ensure it has been defined. DoD has determined atypical usage is not appropriate to define at the Enterprise level.
AC-2 (12)	AC-2 (12) (a)	CCI-002147	The organization monitors information system accounts for organization-defined atypical use.	The organization being inspected/assessed monitors information system accounts for atypical use defined in AC-2 (12), CCI 2146. The organization must maintain an audit trail of monitoring.	The organization conducting the inspection/assessment obtains and examines the audit trail of monitoring to ensure the organization being inspected/assessed monitors information system accounts for atypical use defined in AC-2 (12), CCI 2146.
AC-2 (12)	AC-2 (12) (b)	CCI-002148	The organization defines the personnel or roles to whom atypical usage of information system accounts are to be reported.	DoD has defined the personnel or roles as at a minium, the ISSO.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as at a minium, the ISSO.
AC-2 (12)	AC-2 (12) (b)	CCI-002149	The organization reports atypical usage of information system accounts to organization-defined personnel or roles.	The organization being inspected/assessed documents and implements a process to report atypical usage defined in AC-2 (12), CCI 2146 of information system accounts to at a minium, the ISSO. The organization must maintain an audit trail of reporting. DoD has defined the personnel or roles as at a minium, the ISSO.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of reporting to ensure the organization being inspected/assessed reports atypical usage defined in AC-2 (12), CCI 2146 of information system accounts to at a minium, the ISSO. DoD has defined the personnel or roles as at a minium, the ISSO.
AC-2 (13)	AC-2 (13)	CCI-002150	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.	DoD has defined the time period as 30 minutes unless otherwise defined in formal organizational policy.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as 30 minutes unless otherwise defined in formal organizational policy.
AC-2 (13)	AC-2 (13)	CCI-002151	The organization disables accounts of users posing a significant risk within organization-defined time period of discovery of the risk.	The organization being inspected/assessed documents and implements a process to disable accounts of users posing a significant risk within 30 minutes unless otherwise defined in formal organizational policy. DoD has defined the time period as 30 minutes unless otherwise defined in formal organizational policy.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed disables accounts of users posing a significant risk within 30 minutes unless otherwise defined in formal organizational policy. DoD has defined the time period as 30 minutes unless otherwise defined in formal organizational policy.
AC-3	AC-3	CCI-000213	The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	The organization being inspected/assessed configures the information system to enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 213.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 213.

AC-3 (4)	AC-3 (4)	CCI-002163	The organization defines the discretionary access control policies the information system is to enforce over subjects and objects.	The organization being inspected/assessed defines and documents the discretionary access control policies the information system is to enforce over subjects and objects. DoD has determined that the discretionary access control policies are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented access control policies to ensure they have been defined. DoD has determined that the discretionary access control policies are not appropriate to define at the Enterprise level.
AC-3 (4)	AC-3 (4)	CCI-002164	The organization specifies in the discretionary access control policies that a subject which 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.	The organization being inspected/assessed documents the discretionary access control policies that a subject which 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.	The organization conducting the inspection/assessment obtains and examines the documented discretionary access control policies to ensure the organization being inspected/assessed specifies that a subject which 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.
AC-3 (4)	AC-3 (4)	CCI-002165	The information system enforces organization-defined discretionary access control policies over defined subjects and objects.	The organization being inspected/assessed configures the information system to enforce the discretionary access control policies defined in AC-3 (4), CCI 2163 over defined subjects and objects. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2165.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to enforce the discretionary access control policies defined in AC-3 (4), CCI 2163 over defined subjects and objects. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2165.
AC-5	AC-5 (a)	CCI-002219	The organization defines the duties of individuals that are to be separated.	The organization being inspected/assessed defines and documents the duties of individuals that are to be separated. DoD has determined the duties are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented duties to ensure the organization being inspected/assessed defines the duties of individuals that are to be separated. DoD has determined the duties are not appropriate to define at the Enterprise level.
AC-5	AC-5 (a)	CCI-000036	The organization separates organization-defined duties of individuals.	The organization being inspected/assessed documents and implements processes to maintain separation of the duties defined in AC-5, CCI 2219 across different individuals within the organization.	The organization conducting the inspection/assessment obtains and examines the documented processes to ensure the organization being inspected/assessed maintains separation of the duties defined in AC-5, CCI 2219 across different individuals within the organization.
AC-5	AC-5 (b)	CCI-001380	The organization documents separation of duties of individuals.	The organization being inspected/assessed documents separation of duties of individuals.	The organization conducting the inspection/assessment obtains and examines the documented separation of duties to ensure the organization being inspected/assessed documents separation of duties of individuals.
AC-5	AC-5 (c)	CCI-002220	The organization defines information system access authorizations to support separation of duties.	The organization being inspected/assessed defines and documents the information system access authorizations to support separation of duties.	The organization conducting the inspection/assessment obtains and examines the documented information system access authorizations to ensure the organization being inspected/assessed defines information system access authorizations to support separation of duties.
AC-6	AC-6	CCI-000225	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.	The organization being inspected/assessed documents and implements 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.	The organization conducting the inspection/assessment obtains and examines the documented processes to ensure that the organization being inspected/assessed implements 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.
AC-6 (1)	AC-6 (1)	CCI-001558	The organization defines the security functions (deployed in hardware, software, and firmware) for which access must be explicitly authorized.	DoD has defined the security functions as all functions not publicly accessible.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the security functions as all functions not publicly accessible.
AC-6 (1)	AC-6 (1)	CCI-002221	The organization defines the security-relevant information for which access must be explicitly authorized.	DoD has defined the security-relevant information as all security-relevant information not publicly available.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the security-relevant information as all security-relevant information not publicly available.

AC-6 (1)	AC-6 (1)	CCI-002222	The organization explicitly authorizes access to organization-defined security functions.	The organization being inspected/assessed documents and implements a process to explicitly authorize access to all functions not publicly accessible. Explicit authorization can be in the form of an acceptable use policy signed by the user at the time of access being granted. DoD has defined the security functions as all functions not publicly accessible.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed explicitly authorizes access to all functions not publicly accessible. DoD has defined the security functions as all functions not publicly accessible.
AC-6 (1)	AC-6 (1)	CCI-002223	The organization explicitly authorizes access to organization-defined security-relevant information.	The organization being inspected/assessed documents and implements a process to explicitly authorize access to all security-relevant information not publicly available. Explicit authorization can be in the form of an acceptable use policy signed by the user at the time of access being granted. DoD has defined the security-relevant information as all security-relevant information not publicly available.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed explicitly authorizes access to all security-relevant information not publicly available. DoD has defined the security-relevant information as all security-relevant information not publicly available.
AC-6 (2)	AC-6 (2)	CCI-000039	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.	The organization being inspected/assessed documents and implements a process to require that users of information system accounts or roles, with access to any privileged security functions or security-relevant information, use non-privileged accounts, or roles, when accessing nonsecurity functions. DoD has defined the security functions and security-relevant information as any privileged security functions or security-relevant information.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed requires that users of information system accounts or roles, with access to any privileged security functions or security-relevant information, use non-privileged accounts, or roles, when accessing nonsecurity functions. DoD has defined the security functions and security-relevant information as any privileged security functions or security-relevant information.
AC-6 (2)	AC-6 (2)	CCI-001419	The organization defines the security functions or security-relevant information to which users of information system accounts, or roles, have access.	DoD has defined the security functions and security-relevant information as any privileged security functions or security-relevant information.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the security functions and security-relevant information as any privileged security functions or security-relevant information.
AC-6 (5)	AC-6 (5)	CCI-002226	The organization defines the personnel or roles to whom privileged accounts are to be restricted on the information system.	The organization being inspected/assessed defines and documents the personnel or roles to whom privileged accounts are to be restricted on the information system. DoD has determined the personnel and roles are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented personnel or roles to ensure the organization being inspected/assessed defines the personnel or roles to whom privileged accounts are to be restricted on the information system. DoD has determined the personnel and roles are not appropriate to define at the Enterprise level.
AC-6 (5)	AC-6 (5)	CCI-002227	The organization restricts privileged accounts on the information system to organization-defined personnel or roles.	The organization being inspected/assessed implements a process to only provide privileged accounts on the information system to personnel or roles defined in AC-6 (5), CCI 2226.	The organization conducting the inspection/assessment obtains and examines a sampling of information system access authorizations to ensure the organization being inspected/assessed implements a process to only provide privileged accounts on the information system to personnel or roles defined in AC-6 (5), CCI 2226.
AC-6 (7)	AC-6 (7) (a)	CCI-002228	The organization defines the frequency on which it conducts reviews of the privileges assigned to organization-defined roles or classes of users.	DoD has defined the frequency as at a minimum, annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as at a minimum, annually.
AC-6 (7)	AC-6 (7) (a)	CCI-002229	The organization defines the roles or classes of users that are to have their privileges reviewed on an organization-defined frequency.	DoD has defined the roles or classes of users as all users.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the roles or classes of users as all users.

AC-6 (7)	AC-6 (7) (a)	CCI-002230	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.	The organization being inspected/assessed documents and implements a process to review the privileges assigned to all users at a minimum, annually to validate the need for such privileges. The organization must maintain an audit trail of reviews. DoD has defined the roles or classes of users as all users. DoD has defined the frequency as at a minimum, annually.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of reviews to ensure the organization being inspected/assessed reviews the privileges assigned to all users at a minimum, annually. to validate the need for such privileges. DoD has defined the roles or classes of users as all users. DoD has defined the frequency as at a minimum, annually.
AC-6 (7)	AC-6 (7) (b)	CCI-002331	The organization reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.	The organization being inspected/assessed documents and implements a process to reassign or remove privileges, if necessary, to correctly reflect organizational mission/business needs.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.
AC-6 (8)	AC-6 (8)	CCI-002232	The organization defines software that is restricted from executing at a higher privilege than users executing the software.	DoD has defined the software as any software except software explicitly documented.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the software as any software except software explicitly documented.
AC-6 (8)	AC-6 (8)	CCI-002233	The information system prevents organization-defined software from executing at higher privilege levels than users executing the software.	The organization being inspected/assessed configures the information system to any software except software explicitly documented from executing at higher privilege levels than users executing the software. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2233. DoD has defined the software as any software except software explicitly documented.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to prevent any software except software explicitly documented from executing at higher privilege levels than users executing the software. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2233. DoD has defined the software as any software except software explicitly documented.
AC-6 (9)	AC-6 (9)	CCI-002234	The information system audits the execution of privileged functions.	The organization being inspected/assessed configures the information system to audit the execution of privileged functions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2234.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to audit the execution of privileged functions. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2234.
AC-6 (10)	AC-6 (10)	CCI-002235	The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.	The organization being inspected/assessed configures the information system to prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2235.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2235.
AC-7	AC-7 (a)	CCI-000043	The organization defines the maximum number of consecutive invalid logon attempts to the information system by a user during an organization-defined time period.	DoD has defined the maximum number as three.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the maximum number as three.

AC-7	AC-7 (a)	CCI-000044	The information system enforces the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.	The organization being inspected/assessed configures the information system to limit invalid logon attempts by a user to three attempts during a 15 minute time period. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 44. DoD has defined the maximum number as three. DoD has defined the time period as 15 minutes.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to limit invalid logon attempts by a user to three attempts during a 15 minute time period. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 44. DoD has defined the maximum number as three. DoD has defined the time period as 15 minutes.
AC-7	AC-7 (a)	CCI-001423	The organization defines the time period in which the organization-defined maximum number of consecutive invalid logon attempts occur.	DoD has defined the time period as 15 minutes.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as 15 minutes.
AC-7	AC-7 (b)	CCI-002236	The organization defines the time period the information system will automatically lock the account or node when the maximum number of unsuccessful attempts is exceeded.	DoD has defined the time period as until released by an administrator.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as until released by an administrator.
AC-7	AC-7 (b)	CCI-002237	The organization defines the delay algorithm to be employed by the information system to delay the next login prompt when the maximum number of unsuccessful attempts is exceeded.	DoD has defined the delay algorithm as a minimum of 5 seconds.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the delay algorithm as a minimum of 5 seconds.
AC-7	AC-7 (b)	CCI-002238	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 login prompt according to the organization-defined delay algorithm when the maximum number of unsuccessful attempts is exceeded.	The organization being inspected/assessed configures the information system to automatically lock the account or node until the locked account is released by an administrator and delays the next login prompt for a minimum of 5 seconds when the maximum number of unsuccessful attempts is exceeded. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2238. DoD has defined the delay algorithm as a minimum of 5 seconds. DoD has defined the time period as until released by an administrator.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to automatically lock the account or node until the locked account is released by an administrator and delays the next login prompt for a minimum of 5 seconds when the maximum number of unsuccessful attempts is exceeded. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2238. DoD has defined the delay algorithm as a minimum of 5 seconds. DoD has defined the time period as until released by an administrator.
AC-8	AC-8 (a)	CCI-002247	The organization defines the use notification message or banner the information system displays to users before granting access to the system.	DoD has defined the use notification message or banner as the content of DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the use notification message or banner as the content of DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013.

AC-8	AC-8 (a)	CCI-000048	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.	The organization being inspected/assessed configures the information system to display the DoD Information Systems – Standard Consent Banner and User Agreement 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. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 48. DoD has defined the use notification message or banner as the content of DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to display the DoD Information Systems – Standard Consent Banner and User Agreement 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. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 48. DoD has defined the use notification message or banner as the content of DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013.
AC-8	AC-8 (a) (1)	CCI-002243	The organization-defined information system use notification message or banner is to state that users are accessing a U.S. Government information system.	DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013 meets the DoD requirements the information system use notification message or banner. DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DTM 08-060.	DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013 meets the DoD requirements the information system use notification message or banner. DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DTM 08-060.
AC-8	AC-8 (a) (2)	CCI-002244	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.	DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013 meets the DoD requirements the information system use notification message or banner. DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DTM 08-060.	DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013 meets the DoD requirements the information system use notification message or banner. DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DTM 08-060.
AC-8	AC-8 (a) (3)	CCI-002245	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.	DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013 meets the DoD requirements the information system use notification message or banner. DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DTM 08-060.	DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013 meets the DoD requirements the information system use notification message or banner. DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DTM 08-060.
AC-8	AC-8 (a) (4)	CCI-002246	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.	DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013 meets the DoD requirements the information system use notification message or banner. DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DTM 08-060.	DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013 meets the DoD requirements the information system use notification message or banner. DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DTM 08-060.
AC-8	AC-8 (b)	CCI-000050	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 organization being inspected/assessed configures the information system to retain 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. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 50.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to retain 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. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 50.

AC-8	AC-8 (c) (1)	CCI-001384	The information system, for publicly accessible systems, displays system use information organization-defined conditions before granting further access.	The organization being inspected/assessed configures the information system to display the content of DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems - Standard Consent Banner and User Agreement," March 2013 before granting further access for publicly accessible systems For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1384. DoD has defined the conditions as the content of DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems - Standard Consent Banner and User Agreement," March 2013.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to display the content of DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems - Standard Consent Banner and User Agreement," March 2013 before granting further access for publicly accessible systems For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1384. DoD has defined the conditions as the content of DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems - Standard Consent Banner and User Agreement," March 2013.
AC-8	AC-8 (c) (2)	CCI-001385	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.	The organization being inspected/assessed configures the information system to display references, if any, to monitoring that are consistent with privacy accommodations for such systems that generally prohibit those activities for publicly accessible systems. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1385.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to display references, if any, to monitoring that are consistent with privacy accommodations for such systems that generally prohibit those activities for publicly accessible systems. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1385.
AC-8	AC-8 (c) (2)	CCI-001386	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.	The organization being inspected/assessed configures the information system to display references, if any, to recording that are consistent with privacy accommodations for such systems that generally prohibit those activities for publicly accessible systems. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1386.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to display references, if any, to recording that are consistent with privacy accommodations for such systems that generally prohibit those activities for publicly accessible systems. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1386.
AC-8	AC-8 (c) (2)	CCI-001387	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.	The organization being inspected/assessed configures the information system to display references, if any, to auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities for publicly accessible systems. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1387.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to display references, if any, to auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities for publicly accessible systems. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1387.
AC-8	AC-8 (c) (3)	CCI-001388	The information system, for publicly accessible systems, includes a description of the authorized uses of the system.	The organization being inspected/assessed configures the information system to include a description of the authorized uses of the system for publicly accessible systems. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1388.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to include a description of the authorized uses of the system for publicly accessible systems. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1388.

AC-8	AC-8 (c) (1)	CCI-002248	The organization defines the conditions of use which are to be displayed to users of the information system before granting further access.	DoD has defined the conditions as the content of DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the conditions as the content of DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013.
AC-11	AC-11 (a)	CCI-000059	The organization defines the time period of inactivity after which the information system initiates a session lock.	DoD has defined the time period as 15 minutes.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as 15 minutes.
AC-11	AC-11 (a)	CCI-000058	The information system provides the capability for users to directly initiate session lock mechanisms.	The organization being inspected/assessed configures the information system to provide the capability for users to directly initiate session lock mechanisms. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 58.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to provide the capability for users to directly initiate session lock mechanisms. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 58.
AC-11	AC-11 (b)	CCI-000056	The information system retains the session lock until the user reestablishes access using established identification and authentication procedures.	The organization being inspected/assessed configures the information system to retain the session lock until the user reestablishes access using established identification and authentication procedures. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 56.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to retain the session lock until the user reestablishes access using established identification and authentication procedures. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 56.
AC-11 (1)	AC-11 (1)	CCI-000060	The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.	The organization being inspected/assessed configures the information system to conceal, via the session lock, information previously visible on the display with a publicly viewable image. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 60.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to conceal, via the session lock, information previously visible on the display with a publicly viewable image. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 60.
AC-14	AC-14 (a)	CCI-000061	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.	The organization being inspected/assessed identifies, defines, and documents user actions that can be performed on the information system without identification or authentication consistent with organizational missions/business functions. DoD has determined the user actions are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented user actions to ensure the organization being inspected/assessed identifies and defines the user actions that can be performed on the information system without identification and authentication. DoD has determined the user actions are not appropriate to define at the Enterprise level.
AC-14	AC-14 (b)	CCI-000232	The organization documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification and authentication.	The organization being inspected/assessed documents supporting rationale in the security plan for the actions defined in AC-14, CCI 61 to not require identification and authentication.	The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed documents the supporting rationale for the actions defined in AC-14, CCI 61 to not require identification and authentication.

AC-17	AC-17 (a)	CCI-000063	The organization defines allowed methods of remote access to the information system.	The organization being inspected/assessed defines and documents the allowed methods of remote access to the information system. The methods should be defined IAW ports, protocols, and service requirements, as well as access control requirements for any STIGs applicable to the technology in use. DoD has determined the allowed methods of remote access are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented methods to ensure the organization being inspected/assessed defines allowed methods of remote access to the information system. DoD has determined the allowed methods of remote access are not appropriate to define at the Enterprise level.
AC-17	AC-17 (a)	CCI-002310	The organization establishes and documents usage restrictions for each type of remote access allowed.	The organization being inspected/assessed establishes and documents usage restrictions for each type of remote access allowed.	The organization conducting the inspection/assessment obtains and examines the documented usage restrictions to ensure the organization being inspected/assessed establishes and documents usage restrictions for each type of remote access allowed.
AC-17	AC-17 (a)	CCI-002311	The organization establishes and documents configuration/connection requirements for each type of remote access allowed.	The organization being inspected/assessed establishes and documents configuration/connection requirements for each type of remote access allowed.	The organization conducting the inspection/assessment obtains and examines the documented requirements to ensure the organization being inspected/assessed establishes and documents configuration/connection requirements for each type of remote access allowed.
AC-17	AC-17 (a)	CCI-002312	The organization establishes and documents implementation guidance for each type of remote access allowed.	The organization being inspected/assessed establishes and documents implementation guidance for each type of remote access allowed.	The organization conducting the inspection/assessment obtains and examines the documented implementation guidance to ensure the organization being inspected/assessed establishes and documents implementation guidance for each type of remote access allowed.
AC-17	AC-17 (b)	CCI-000065	The organization authorizes remote access to the information system prior to allowing such connections	The organization being inspected/assessed authorizes remote access to the information system prior to allowing such connections. The organization must maintain an audit trail of authorizations.	The organization conducting the inspection/assessment obtains and examines the audit trail of authorizations to ensure the organization being inspected/assessed authorizes remote access to the information system prior to allowing such connections.
AC-17 (1)	AC-17 (1)	CCI-000067	The information system monitors remote access methods.	The organization being inspected/assessed configures the information system to monitor remote access methods. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 67.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to monitor remote access methods. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 67.
AC-17 (1)	AC-17 (1)	CCI-002314	The information system controls remote access methods.	The organization being inspected/assessed configures the information system to control remote access methods. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2314.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to control remote access methods. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2314.
AC-17 (2)	AC-17 (2)	CCI-000068	The information system implements cryptographic mechanisms to protect the confidentiality of remote access sessions.	The organization being inspected/assessed configures the information system to implement cryptographic mechanisms to protect the confidentiality of remote access sessions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 68.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement cryptographic mechanisms to protect the confidentiality of remote access sessions. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 68.

AC-17 (2)	AC-17 (2)	CCI-001453	The information system implements cryptographic mechanisms to protect the integrity of remote access sessions.	The organization being inspected/assessed configures the information system to implement cryptographic mechanisms to protect the integrity of remote access sessions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1453.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement cryptographic mechanisms to protect the integrity of remote access sessions. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1453.
AC-17 (3)	AC-17 (3)	CCI-001561	The organization defines managed access control points for remote access to the information system.	The organization being inspected/assessed defines and documents managed access control points for remote access to the information system.	The organization conducting the inspection/assessment obtains and examines the documented managed access points to ensure the organization being inspected/assessed defines managed access control points for remote access to the information system.
AC-17 (3)	AC-17 (3)	CCI-002315	The organization defines the number of managed network access control points through which the information system routes all remote access.	The organization being inspected/assessed defines and documents the number of managed network access control points through which the information system routes all remote access. DoD has determined the number is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented number to ensure the organization being inspected/assessed defines the number of managed network access control points through which the information system routes all remote access. DoD has determined the number is not appropriate to define at the Enterprise level.
AC-17 (3)	AC-17 (3)	CCI-000069	The information system routes all remote accesses through organization-defined number managed network access control points.	The organization being inspected/assessed configures the information system to route all remote accesses through the number of managed network access control points defined in AC-17 (3), CCI 2315. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 69.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to route all remote accesses through the number of managed network access control points defined in AC-17 (3), CCI 2315. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 69.
AC-17 (4)	AC-17 (4) (a)	CCI-000070	The organization authorizes the execution of privileged commands via remote access only for organization-defined needs.	The organization being inspected/assessed authorizes the execution of privileged commands via remote access only for needs defined in AC-17 (4), CCI 2317. The organization being inspected/assessed maintains an audit trail of authorizations.	The organization conducting the inspection/assessment obtains and examines the audit trail of authorizations to ensure the organization being inspected/assessed authorizes the execution of privileged commands via remote access only for needs defined in AC-17 (4), CCI 2317.
AC-17 (4)	AC-17 (4) (a)	CCI-002316	The organization authorizes the access to security-relevant information via remote access only for organization-defined needs.	The organization being inspected/assessed authorizes the access to security-relevant information via remote access only for needs defined in AC-17 (4), CCI 2318. The organization being inspected/assessed maintains an audit trail of authorizations.	The organization conducting the inspection/assessment obtains and examines the audit trail of authorizations to ensure the organization being inspected/assessed authorizes the access to security-relevant information via remote access only for needs defined in AC-17 (4), CCI 2318.
AC-17 (4)	AC-17 (4) (a)	CCI-002317	The organization defines the operational needs when the execution of privileged commands via remote access is to be authorized.	The organization being inspected/assessed defines and documents the operational needs when the execution of privileged commands via remote access is to be authorized. DoD has determined the operational needs are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented operational needs to ensure the organization being inspected/assessed defines the operational needs when the execution of privileged commands via remote access is to be authorized. DoD has determined the operational needs are not appropriate to define at the Enterprise level.
AC-17 (4)	AC-17 (4) (a)	CCI-002318	The organization defines the operational needs when access to security-relevant information via remote access is to be authorized.	The organization being inspected/assessed defines and documents the operational needs when access to security-relevant information via remote access is to be authorized. DoD has determined the operational needs are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented operational needs to ensure the organization being inspected/assessed defines the operational needs when access to security-relevant information via remote access is to be authorized. DoD has determined the operational needs are not appropriate to define at the Enterprise level.
AC-17 (4)	AC-17 (4) (b)	CCI-002319	The organization documents in the security plan for the information system the rationale for authorization of the execution of privilege commands via remote access.	The organization being inspected/assessed documents in the security plan for the information system the rationale for authorization of the execution of privilege commands via remote access.	The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed documents in the security plan for the information system the rationale for authorization of the execution of privilege commands via remote access.

AC-17 (4)	AC-17 (4) (b)	CCI-002320	The organization documents in the security plan for the information system the rationale for authorization of access to security-relevant information via remote access.	The organization being inspected/assessed documents in the security plan for the information system the rationale for authorization of access to security-relevant information via remote access.	The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed documents in the security plan for the information system the rationale for authorization of access to security-relevant information via remote access.
AC-17 (6)	AC-17 (6)	CCI-000072	The organization ensures that users protect information about remote access mechanisms from unauthorized use and disclosure.	The organization being inspected/assessed implements and documents a process to ensure that users protect information about remote access mechanisms from unauthorized use and disclosure.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure that the organization being inspected/assessed ensures that users protect information about remote access mechanisms from unauthorized use and disclosure.
AC-17 (9)	AC-17 (9)	CCI-002321	The organization defines the time period within which it disconnects or disables remote access to the information system.	DoD has defined the time period as immediately.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as immediately.
AC-17 (9)	AC-17 (9)	CCI-002322	The organization provides the capability to expeditiously disconnect or disable remote access to the information system within the organization-defined time period.	The organization being inspected/assessed configures the information system to provide the capability to expeditiously disconnect or disable remote access to the information system immediately. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2322. DoD has defined the time period as immediately.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to provide the capability to expeditiously disconnect or disable remote access to the information system immediately. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2322. DoD has defined the time period as immediately.
AC-18	AC-18 (a)	CCI-001438	The organization establishes usage restrictions for wireless access.	The organization being inspected/assessed establishes and documents usage restrictions for wireless access.	The organization conducting the inspection/assessment obtains and examines documented usage restrictions to ensure the organization being inspected/assessed establishes usage restrictions for wireless access.
AC-18	AC-18 (a)	CCI-002323	The organization establishes configuration/connection requirements for wireless access.	The organization being inspected/assessed establishes and documents configuration/connection requirements for wireless access.	The organization conducting the inspection/assessment obtains and examines the documented configuration/connection requirements to ensure the organization being inspected/assessed establishes configuration/connection requirements for wireless access.
AC-18	AC-18 (a)	CCI-001439	The organization establishes implementation guidance for wireless access.	The organization being inspected/assessed establishes and documents implementation guidance for wireless access.	The organization conducting the inspection/assessment obtains and examines the documented implementation guidance to ensure the organization being inspected/assessed establishes implementation guidance for wireless access.
AC-18	AC-18 (b)	CCI-001441	The organization authorizes wireless access to the information system prior to allowing such connections.	The organization being inspected/assessed authorizes wireless access to the information system prior to allowing such connections. The organization must maintain an audit trail of authorizations.	The organization conducting the inspection/assessment obtains and examines the audit trail of authorizations to ensure the organization being inspected/assessed authorizes wireless access to the information system prior to allowing such connections.
AC-18 (1)	AC-18 (1)	CCI-001443	The information system protects wireless access to the system using authentication of users and/or devices.	The organization being inspected/assessed configures the information system to protect wireless access to the system using authentication of users and/or devices. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1443.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to protect wireless access to the system using authentication of users and/or devices. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1443.
AC-18 (1)	AC-18 (1)	CCI-001444	The information system protects wireless access to the system using encryption.	The organization being inspected/assessed configures the information system to protect wireless access to the system using encryption. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1444.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to protect wireless access to the system using encryption. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1444.

AC-18 (3)	AC-18 (3)	CCI-001449	The organization disables, when not intended for use, wireless networking capabilities internally embedded within information system components prior to issuance and deployment.	The organization being inspected/assessed documents and implements a process to disable wireless networking capabilities internally embedded within information system components prior to issuance and deployment when not intended for use.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed disables, when not intended for use, wireless networking capabilities internally embedded within information system components prior to issuance and deployment. The organization conducting the inspection/assessment obtains and examines a sampling of information systems to ensure that any internally embedded wireless networking capabilities are disabled unless a documented need exists.
AC-18 (4)	AC-18 (4)	CCI-002324	The organization identifies and explicitly authorizes users allowed to independently configure wireless networking capabilities.	The organization being inspected/assessed identifies and explicitly authorizes users allowed to independently configure wireless networking capabilities. The organization must maintain an audit trail of authorizations.	The organization conducting the inspection/assessment obtains and examines the audit trail of authorizations to ensure the organization being inspected/assessed identifies and explicitly authorizes users allowed to independently configure wireless networking capabilities.
AC-19	AC-19 (a)	CCI-000082	The organization establishes usage restrictions for organization controlled mobile devices.	The organization being inspected/assessed establishes and documents usage restrictions for organization controlled mobile devices.	The organization conducting the inspection/assessment obtains and examines the documented usage restrictions to ensure the organization being inspected/assessed establishes usage restrictions for organization controlled mobile devices.
AC-19	AC-19 (a)	CCI-002325	The organization establishes configuration requirements for organization controlled mobile devices.	DoD is automatically compliant with this CCI because existing STIGs establish configuration requirements for approved mobile devices.	DoD is automatically compliant with this CCI because existing STIGs establish configuration requirements for approved mobile devices.
AC-19	AC-19 (a)	CCI-002326	The organization establishes connection requirements for organization controlled mobile devices.	The organization being inspected/assessed establishes and documents connection requirements for organization controlled mobile devices.	The organization conducting the inspection/assessment obtains and examines the documented connection requirements to ensure the organization being inspected/assessed establishes connection requirements for organization controlled mobile devices.
AC-19	AC-19 (a)	CCI-000083	The organization establishes implementation guidance for organization controlled mobile devices.	The organization being inspected/assessed establishes and documents implementation guidance for organization controlled mobile devices.	The organization conducting the inspection/assessment obtains and examines the documented implementation guidance to ensure the organization being inspected/assessed establishes implementation guidance for organization controlled mobile devices.
AC-19	AC-19 (b)	CCI-000084	The organization authorizes connection of mobile devices to organizational information systems.	The organization being inspected/assessed authorizes connection of mobile devices to organizational information systems. The organization must maintain an audit trail of authorizations.	The organization conducting the inspection/assessment obtains and examines the audit trail of authorizations to ensure the organization being inspected/assessed authorizes connection of mobile devices to organizational information systems.
AC-20	AC-20 (a)	CCI-000093	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.	The organization being inspected/assessed establishes and documents 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.	The organization conducting the inspection/assessment obtains and examines the documented terms and conditions to ensure the organization being inspected/assessed 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.
AC-20	AC-10 (b)	CCI-002332	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.	The organization being inspected/assessed establishes and documents the 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.	The organization conducting the inspection/assessment obtains and examines the documented terms and conditions to ensure the organization being inspected/assessed 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.
AC-20 (1)	AC-20 (1) (a)	CCI-002333	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.	The organization being inspected/assessed documents and implements a process to permit 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.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed 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.

AC-20 (1)	AC-20 (1) (a)	CCI-002334	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.	The organization being inspected/assessed documents and implements a process to permit 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.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed 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.
AC-20 (1)	AC-20 (1) (a)	CCI-002335	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.	The organization being inspected/assessed documents and implements a process to permit 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.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed 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.
AC-20 (1)	AC-20 (1) (a)	CCI-002336	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.	The organization being inspected/assessed documents and implements a process to permit 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.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed 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.
AC-20 (1)	AC-20 (1) (b)	CCI-002337	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.	The organization being inspected/assessed documents and implements a process to permit 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.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed 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.
AC-20 (2)	AC-20 (2)	CCI-000097	The organization restricts or prohibits the use of organization-controlled portable storage devices by authorized individuals on external information systems.	The organization being inspected/assessed	The organization conducting the inspection/assessment obtains and examines
AC-20 (3)	AC-20 (3)	CCI-002338	The organization restricts or prohibits the use of non-organizationally owned information systems, system components, or devices to process, store, or transmit organizational information.	The organization being inspected/assessed documents and implements a process to restrict or prohibit the use of non-organizationally owned information systems, system components, or devices to process, store, or transmit organizational information.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed restricts or prohibits the use of non-organizationally owned information systems, system components, or devices to process, store, or transmit organizational information.
AC-22	AC-22 (a)	CCI-001473	The organization designates individuals authorized to post information onto a publicly accessible information system.	The organization being inspected/assessed identifies and documents individuals authorized to post information onto a publicly accessible information system.	The organization conducting the inspection/assessment obtains and examines the list of individuals to ensure the organization being inspected/assessed designates individuals authorized to post information onto a publicly accessible information system.
AC-22	AC-22 (b)	CCI-001474	The organization trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information.	The organization being inspected/assessed documents and implements a process to train authorized individuals to ensure that publicly accessible information does not contain nonpublic information. The organization must maintain an audit trail of the training conducted.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of the training conducted to ensure the organization being inspected/assessed trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information.
AC-22	AC-22 (c)	CCI-001475	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.	The organization being inspected/assessed	The organization conducting the inspection/assessment obtains and examines
AC-22	AC-22 (d)	CCI-001476	The organization reviews the content on the publicly accessible information system for nonpublic information on an organization-defined frequency.	The organization being inspected/assessed documents and implements a process to review the content on the publicly accessible information system for nonpublic information on an organization-defined frequency. The organization must maintain an audit trail of reviews.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of reviews to ensure the organization being inspected/assessed reviews the content on the publicly accessible information system for nonpublic information on an organization-defined frequency.

AC-22	AC-22 (d)	CCI-001477	The organization defines a frequency for reviewing the content on the publicly accessible information system for nonpublic information.	DoD has defined the frequency as every 90 days or as new information is posted.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every 90 days or as new information is posted.
AC-22	AC-22 (e)	CCI-001478	The organization removes nonpublic information from the publicly accessible information system, if discovered.	The organization being inspected/assessed documents and implements a process to remove nonpublic information from the publicly accessible information system, if discovered.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed removes nonpublic information from the publicly accessible information system, if discovered.
AT-1	AT-1 (a)	CCI-002048	The organization defines the personnel or roles to whom the security awareness and training policy is disseminated.	DoD has defined the roles as organizational personnel with security awareness and training responsibilities. DoD disseminates DoDD 8570.01 organization-wide via the DoD Issuances website. http://www.dtic.mil/whs/directives/corres/dir.html	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the roles as organizational personnel with security awareness and training responsibilities.
AT-1	AT-1 (a)	CCI-002049	The organization defines the personnel or roles to whom the security awareness and training procedures are disseminated.	DoD has defined the roles as organizational personnel with security awareness and training responsibilities.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the roles as organizational personnel with security awareness and training responsibilities.
AT-1	AT-1 (a) (1)	CCI-000100	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.	DoDD 8570.01 meets the DoD requirement for IA awareness training policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01. Comment: DoDD 8570.01 will be updated with DoDD 8140 once signed. The organization's use of their higher command policy/procedures meets this requirement if more stringent.	DoDD 8570.01 meets the DoD requirement for IA awareness training policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01. Comment: The organization's use of their higher command policy/procedures meets this requirement if more stringent.
AT-1	AT-1 (a) (1)	CCI-000101	The organization disseminates a security awareness and training policy to organization-defined personnel or roles.	DoD disseminates DoDD 8570.01 organization-wide via the DoD Issuances website. http://www.dtic.mil/whs/directives/corres/dir.html	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01.
AT-1	AT-1 (a) (2)	CCI-000103	The organization develops and documents procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.	DoD develops and documents procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls within DoDD 8570.01. DISA's DoD IA awareness CBT is the DoD baseline standard. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01.	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01.
AT-1	AT-1 (a) (2)	CCI-000104	The organization disseminates security awareness and training procedures to organization-defined personnel or roles.	DoD disseminates DoDD 8570.01 organization-wide via the DoD Issuances website. http://www.dtic.mil/whs/directives/corres/dir.html DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01. DoD has defined the roles as organizational personnel with security awareness and training responsibilities.	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01. DoD has defined the roles as organizational personnel with security awareness and training responsibilities.
AT-1	AT-1 (b) (1)	CCI-000102	The organization reviews and updates the current security awareness and training policy in accordance with organization-defined frequency.	DoDD 8570.01 meets the DoD requirement for IA awareness training policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01.	DoDD 8570.01 meets the DoD requirement for IA awareness training policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01.
AT-1	AT-1 (b) (1)	CCI-001564	The organization defines the frequency of security awareness and training policy reviews and updates.	DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.

AT-1	AT-1 (b) (2)	CCI-000105	The organization reviews and updates the current security awareness and training procedures in accordance with organization-defined frequency.	The organization conducting the inspection/assessment obtains and examines the audit trail of reviews and updates to ensure the organization being inspected/assessed reviews and updates the current security awareness and training procedures annually. DoD has defined the frequency as annually.	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01. DoD has defined the frequency as annually.
AT-1	AT-1 (b) (2)	CCI-001565	The organization defines the frequency of security awareness and training procedure reviews and updates.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as reviewed annually - updated as appropriate.
AT-2	AT-2	CCI-001480	The organization defines the frequency for providing refresher security awareness training to all information system users (including managers, senior executives, and contractors).	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level (DoDD 8570.01). DoD has defined the frequency as annually.
AT-2	AT-2 (a)	CCI-000106	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.	DoDD 8570.01 meets the DoD requirement for IA awareness training policy and procedures. DISA's DoD IA awareness CBT is the DoD baseline standard. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01.	DoDD 8570.01 meets the DoD requirement for IA awareness training policy and procedures. DISA's DoD IA awareness CBT is the DoD baseline standard. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01.
AT-2	AT-2 (b)	CCI-000112	The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors) when required by information system changes.	DoDD 8570.01 meets the DoD requirement for IA awareness training policy and procedures. DISA's DoD IA awareness CBT is the DoD baseline standard. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01.	DoDD 8570.01 meets the DoD requirement for IA awareness training policy and procedures. DISA's DoD IA awareness CBT is the DoD baseline standard. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01.
AT-2	AT-2 (c)	CCI-001479	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.	DoDD 8570.01 meets the DoD requirement for IA awareness training policy and procedures. DISA's DoD IA awareness CBT is the DoD baseline standard. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01.	DoDD 8570.01 meets the DoD requirement for IA awareness training policy and procedures. DISA's DoD IA awareness CBT is the DoD baseline standard. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01.
AT-2 (2)	AT-2 (2)	CCI-002055	The organization includes security awareness training on recognizing and reporting potential indicators of insider threat.	The IA Awareness CBT, "Cyber Awareness Challenge," and Virtual Training Environment (VTE) Courses: "Introduction to Insider Threat" and "Monitoring for Insider Threat" available on the IASE website meet the DoD requirement to include security awareness training on recognizing and reporting potential indicators of insider threat. DoD Components are automatically compliant with this CCI because they are covered by the DoD level training available on the IASE website.	The IA Awareness CBT, "Cyber Awareness Challenge," and Virtual Training Environment (VTE) Courses: "Introduction to Insider Threat" and "Monitoring for Insider Threat" available on the IASE website meet the DoD requirement to include security awareness training on recognizing and reporting potential indicators of insider threat. DoD Components are automatically compliant with this CCI because they are covered by the DoD level training available on the IASE website.
AT-3	AT-3 (a)	CCI-000108	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	DoDD 8570.01 meets the DoD requirement for IA awareness training policy and procedures. DISA's DoD IA awareness CBT for privileged users is the DoD baseline standard. DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDD 8570.01. .	DoDD 8570.01 meets the DoD requirement for IA awareness training policy and procedures. DISA's DoD IA awareness CBT for privileged users is the DoD baseline standard. DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDD 8570.01.
AT-3	AT-3 (b)	CCI-000109	The organization provides role-based security training to personnel with assigned security roles and responsibilities when required by information system changes.	Privileged user type Security-related education/training available through DISA IASE (e.g. VTE, Skill Soft, other professional sources) meets the provision of this control. The organization being inspected/assessed may define specific requirements within the above listed sources for their personnel.	The organization conducting the inspection/assessment obtains and examines documented records (IAW AT-4) of their privileged users training.

AT-3	AT-3 (c)	CCI-000110	The organization provides refresher role-based security training to personnel with assigned security roles and responsibilities in accordance with organization-defined frequency.	Privileged user type Security-related education/training available through DISA IASE (e.g. VTE, Skill Soft, other professional sources) meets the provision of this control. The organization being inspected/assessed may define specific requirements within the above listed sources for their personnel.	The organization conducting the inspection/assessment obtains and examines documented records (IAW AT-4) of their privileged users training.
AT-3	AT-3 (c)	CCI-000111	The organization defines a frequency for providing refresher role-based security training.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.
AT-3 (2)	AT-3 (2)	CCI-001568	The organization defines a frequency for providing employees with refresher training in the employment and operation of physical security controls.	DoD has defined the frequency as annual.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annual.
AT-3 (2)	AT-3 (2)	CCI-002051	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.	The organization being inspected/assessed defines and documents the personnel or roles to whom initial and refresher training in the employment and operation of physical security controls is to be provided. DoD has determined the personnel or roles are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented personnel or roles to ensure the organization being inspected/assessed defines the personnel or roles to whom initial and refresher training in the employment and operation of physical security controls is to be provided. DoD has determined the personnel or roles are not appropriate to define at the Enterprise level.
AT-3 (2)	AT-3 (2)	CCI-001566	The organization provides organization-defined personnel or roles with initial training in the employment and operation of physical security controls.	The organization being inspected/assessed: 1. Identifies and documents physical security controls that require training. 2. Identifies the personnel defined in AT-3 (2), CCI 2051 3. Ensures designated personnel receive this training. 4. Maintains and monitors records of personnel who have received this training.	The organization conducting the inspection/assessment obtains and examines: 1. Documentation of physical security controls that require training. 2. Documented list of personnel defined in AT-3 (2), CCI 2051 3. Ensures identified personnel have received the initial training.
AT-3 (2)	AT-3 (2)	CCI-001567	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.	The organization being inspected/assessed: 1. Identifies and documents physical security controls that require training. 2. Identifies personnel defined in AT-3 (2), CCI 2051 3. Ensures designated personnel receive this training annually 4. Maintains and monitors records of personnel who have received this training. DoD has defined the frequency as annual.	The organization conducting the inspection/assessment obtains and examines: 1. Documentation of physical security controls that require training. 2. Documented list of personnel defined in AT-3 (2), CCI 2051 3. Ensures identified personnel have received training annually. DoD has defined the frequency as annual.
AT-3 (4)	AT-3 (4)	CCI-002053	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.	The organization being inspected/assessed provides training to its personnel on indicators of malicious code defined in AT-3 (4), CCI 2054 to recognize suspicious communications and anomalous behavior in organizational information systems.	The organization conducting the inspection/assessment obtains and examines the training materials and indicators of malicious code defined in AT-3 (4), CCI 2054 to ensure the organization being inspected/assessed provides users with the means to recognize suspicious communications and anomalous behavior in organizational information systems.
AT-3 (4)	AT-3 (4)	CCI-002054	The organization defines indicators of malicious code to recognize suspicious communications and anomalous behavior in organizational information systems.	The organization being inspected/assessed defines and documents indicators of malicious code to recognize suspicious communications and anomalous behavior in organizational information systems. DoD has determined the indicators are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented indicators to ensure the organization being inspected/assessed defines indicators of malicious code to recognize suspicious communications and anomalous behavior in organizational information systems. DoD has determined the indicators are not appropriate to define at the Enterprise level.
AT-4	AT-4 (a)	CCI-000113	The organization documents individual information system security training activities, including basic security awareness training and specific information system security training.	The organization being inspected/assessed identifies and documents training activities to include basic security awareness training (per AT-2) and role-based security related training (per AT-3) IAW DoD 8570.01M.	The organization conducting the inspection/assessment obtains and examines the security awareness training activities to ensure the organization being inspected/assessed documents training activities to include basic security awareness training (per AT-2) and role-based security related training (per AT-3) IAW DoD 8570.01M.
AT-4	AT-4 (a)	CCI-000114	The organization monitors individual information system security training activities, including basic security awareness training and specific information system security training.	The organization being inspected/assessed maintains and monitors records identifying personnel who have received training and the date the training was received	The organization conducting the inspection/assessment obtains and examines records identifying personnel who have received training and the date the training was received

AT-4	AT-4 (b)	CCI-001336	The organization retains individual training records for an organization-defined time period.	The organization being inspected/assessed will maintain records training records for at least 5 years or 5 years after completion of a specific training program. DoD has defined the frequency as at least 5 years or 5 years after completion of a specific training program.	The organization conducting the inspection/assessment obtains and examines training records to ensure records have been maintained for at least 5 years or 5 years after completion of a specific training program. DoD has defined the frequency as at least 5 years or 5 years after completion of a specific training program.
AT-4	AT-4 (b)	CCI-001337	The organization defines a time period for retaining individual training records.	DoD has defined the frequency as at least 5 years or 5 years after completion of a specific training program.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as at least 5 years or 5 years after completion of a specific training program.
AU-1	AU-1 (a)	CCI-001930	The organization defines the organizational personnel or roles to whom the audit and accountability policy is to be disseminated.	The organization being inspected/assessed defines and documents any personnel or roles, in addition to the ISSO or ISSM, to whom the audit and accountability policy is to be disseminated. If there are no additional personnel or roles, the organization must also document that. DoD has defined the personnel or roles as the ISSO and ISSM and others as the local organization deems appropriate.	The organization conducting the inspection/assessment obtains and examines the documented list of personnel or roles to whom the audit and accountability policy is to be disseminated to ensure the organization being inspected/assessed has either defined additional personnel or roles, or identified that there are no additional personnel or roles. DoD has defined the personnel or roles as the ISSO and ISSM and others as the local organization deems appropriate.
AU-1	AU-1 (a)	CCI-001931	The organization defines the organizational personnel or roles to whom the audit and accountability procedures are to be disseminated.	The organization being inspected/assessed defines and documents any personnel or roles, in addition to the ISSO or ISSM, to whom the audit and accountability procedures are to be disseminated. If there are no additional personnel or roles, the organization must also document that. DoD has defined the personnel or roles as the ISSO and ISSM and others as the local organization deems appropriate.	The organization conducting the inspection/assessment obtains and examines the documented list of personnel or roles to whom the audit and accountability procedures are to be disseminated to ensure the organization being inspected/assessed has either defined additional personnel or roles, or identified that there are no additional personnel or roles. DoD has defined the personnel or roles as the ISSO and ISSM and others as the local organization deems appropriate.
AU-1	AU-1 (a) (1)	CCI-000117	The organization develops and documents an audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	The organization being inspected/assessed develops and documents an audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	The organization conducting the inspection/assessment obtains and examines the audit and accountability policy to ensure that the audit and accountability policy addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
AU-1	AU-1 (a) (1)	CCI-001832	The organization disseminates the audit and accountability policy to organization-defined personnel or roles.	The organization being inspected/assessed disseminates, via an information sharing capibility, to the ISSO and ISSM and others as the local organization deems appropriate an audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. DoD has defined the personnel or roles as the ISSO and ISSM and others as the local organization deems appropriate.	The organization conducting the inspection/assessment obtains and examines the audit and accountability procedures via the inspected organization's information sharing capability (e.g. portal, intranet, email, etc.) to ensure it has been disseminated.
AU-1	AU-1 (a) (2)	CCI-000120	The organization develops and documents procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.	The organization being inspected/assessed develops and documents procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.	The organization conducting the inspection/assessment obtains and examines the audit and accountability procedures to ensure that the procedures facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.
AU-1	AU-1 (a) (2)	CCI-001834	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.	The organization being inspected/assessed disseminates, via an information sharing capibility, to the ISSO and ISSM and others as the local organization deems appropriate audit and accountability procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls. DoD has defined the personnel or roles as the ISSO and ISSM and others as the local organization deems appropriate.	The organization conducting the inspection/assessment obtains and examines the audit and accountability procedures via the inspected organization's information sharing capability (e.g. portal, intranet, email, etc.) to ensure it has been disseminated.

AU-1	AU-1 (b) (1)	CCI-000119	The organization reviews and updates the audit and accountability policy on an organization-defined frequency.	The organization being inspected/assessed reviews and updates the audit and accountability policy annually. The organization must maintain an audit trail of reviews and updates. Any changes or acceptance of the document without change must be captured in the audit trail. DoD has defined the frequency as annually.	The organization conducting the inspection/assessment obtains and examines the audit trail of reviews and updates to ensure the organization being inspected/assessed reviews and updates the audit and accountability policy annually. DoD has defined the frequency as annually.
AU-1	AU-1 (b) (1)	CCI-001569	The organization defines the frequency on which it will review and update the audit and accountability policy.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.
AU-1	AU-1 (b) (2)	CCI-000122	The organization reviews and updates the audit and accountability procedures on an organization-defined frequency.	The organization being inspected/assessed reviews and updates the audit and accountability procedures annually. The organization must maintain an audit trail of reviews and updates. Any changes or acceptance of the document without change must be captured in the audit trail. DoD has defined the frequency as annually.	The organization conducting the inspection/assessment obtains and examines the audit trail of reviews and updates to ensure the organization being inspected/assessed reviews and updates the audit and accountability procedures annually. DoD has defined the frequency as annually.
AU-1	AU-1 (b) (2)	CCI-001570	The organization defines the frequency on which it will review and update the audit and accountability procedures.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.
AU-2	AU-2 (a)	CCI-000123	The organization determines the information system must be capable of auditing an organization-defined list of auditable events.	The organization being inspected/assessed determines whether the information system is capable of auditing: - successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g. Classification levels), - Successful and unsuccessful logon attempts, - Privileged activities or other system level access, - Starting and ending time for user access to the system, - Concurrent logons from different workstations, - Successful and unsuccessful accesses to objects, - All program initiations, - All direct access to the information system, - All account creations, modifications, disabling, and terminations, - All kernel module load, unload, and restart. The organization must document those auditable events that are not captured.	The organization conducting the inspection/assessment obtains and examines the documentation of the auditable events to ensure the information system is capable of auditing the: - successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g. Classification levels), - Successful and unsuccessful logon attempts, - Privileged activities or other system level access, - Starting and ending time for user access to the system, - Concurrent logons from different workstations, - Successful and unsuccessful accesses to objects, - All program initiations, - All direct access to the information system, - All account creations, modifications, disabling, and terminations, - All kernel module load, unload, and restart. DoD has defined the information system auditable events as successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g. classification levels). Successful and unsuccessful logon attempts, Privileged activities or other system level access, Starting and ending time for user access to the system, Concurrent logons from different workstations, Successful and
AU-2	AU-2 (a)	CCI-001571	The organization defines the information system auditable events.	DoD has defined the information system auditable events as successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g. classification levels). Successful and unsuccessful logon attempts, Privileged activities or other system level access, Starting and ending time for user access to the system, Concurrent logons from different workstations, Successful and unsuccessful accesses to objects, All program initiations, All direct access to the information system. All account creations, modifications, disabling, and terminations. All kernel module load, unload, and restart.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the information system auditable events as successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g. classification levels). Successful and unsuccessful logon attempts, Privileged activities or other system level access, Starting and ending time for user access to the system, Concurrent logons from different workstations, Successful and unsuccessful accesses to objects, All program initiations, All direct access to the information system. All account creations, modifications, disabling, and terminations. All kernel module load, unload, and restart.
AU-2	AU-2 (b)	CCI-000124	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.	The organization being inspected/assessed documents and implements within the audit and accountability policy and procedures, a process to coordinate the additional auditable events. The objective is to enhance mutual support and to help guide the selection of auditable events. The organization must maintain artifacts of the coordination.	The organization conducting the inspection/assessment obtains and examines the audit and accountability policy and procedures as well as artifacts of the coordination to determine if coordination is necessary and if necessary, whether it has been performed.

AU-2	AU-2 (c)	CCI-000125	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.	The organization being inspected/assessed documents in the audit and accountability policy the list of auditable system events, the organization provides clearly stated rationale for the selection of each system event. The rationale will support any after-action investigations of security event.	The organization conducting the inspection/assessment obtains and examines the audit and accountability policy and procedures to ensure the organization being inspected/assess has defined the auditable system events, rationale for the selection, and that the organization has defined how the auditable events will support after-action investigations of security events.
AU-2	AU-2 (d)	CCI-001485	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.	The organization being inspected/assessed defines and documents events which are to be audited on the information system. Events should be selected from the events the information system is capable of auditing as defined in AU-2 (a) and should be based on ongoing risk assessments of current threat information and environment. DoD has determined that the events are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented list of events which are to be audited on the information system to ensure those events have been defined. DoD has determined that the events are not appropriate to define at the Enterprise level.
AU-2	AU-2 (d)	CCI-001484	The organization defines frequency of (or situation requiring) auditing for each identified event.	DoD has defined the frequency as all auditable events defined in AU-2 (a) per occurrence.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as all auditable events defined in AU-2 (a) per occurrence.
AU-2	AU-2 (d)	CCI-000126	The organization determines that the organization-defined subset of the auditable events defined in AU-2 are to be audited within the information system.	The organization conducting the inspection/assessment reviews the documented audit process as well as audit logs to ensure that the organization being inspected/assessed audits all auditable events defined in AU-2 (a) per occurrence. DoD has defined the actions as all auditable events defined in AU-2 (a) per occurrence.	The organization conducting the inspection/assessment reviews the documented audit process as well as audit logs to ensure that the organization being inspected/assessed audits all auditable events defined in AU-2 (a) per occurrence. DoD has defined the actions as all auditable events defined in AU-2 (a) per occurrence.
AU-2 (3)	AU-2 (3)	CCI-000127	The organization reviews and updates the list of organization-defined audited events on an organization-defined frequency.	The organization being inspected/assessed will conduct reviews of the list of auditable events as defined in AU-2 (d), CCI 1485 annually or more frequently upon changes to situational awareness of threats or vulnerabilities. The organization will generate and maintain an audit trail to document the completion of the review and update actions. DoD has defined the frequency as annually or more frequently upon changes to situational awareness of threats or vulnerabilities.	The organization conducting the inspection/assessment reviews the audit trail showing reviews and updates to the list of audited events to ensure that the list is reviewed and updated annually or more frequently upon changes to situational awareness of threats or vulnerabilities. DoD has defined the frequency as annually or more frequently upon changes to situational awareness of threats or vulnerabilities.
AU-2 (3)	AU-2 (3)	CCI-001486	The organization defines a frequency for reviewing and updating the list of organization-defined auditable events.	DoD has defined the frequency as annually or more frequently upon changes to situational awareness of threats or vulnerabilities.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually or more frequently upon changes to situational awareness of threats or vulnerabilities.
AU-3	AU-3	CCI-000130	The information system generates audit records containing information that establishes what type of event occurred.	The organization being inspected/assessed configures the information system to generate audit records containing information that establishes what type of event occurred For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 130.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed has configured the information system to generate audit records containing information that establishes what type of event occurred. The organization conducting the inspection/assessment reviews the audit records generated to ensure that the records contain information that establishes what type of event occurred. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 130.

AU-3	AU-3	CCI-000131	The information system generates audit records containing information that establishes when an event occurred.	The organization being inspected/assessed configures the information system to generate audit records containing information that establishes when an event occurred For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 131.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed has configured the information system to generate audit records containing information that establishes when an event occurred. The organization conducting the inspection/assessment reviews the audit records generated to ensure that the records contain information that establishes when an event occurred. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 131.
AU-3	AU-3	CCI-000132	The information system generates audit records containing information that establishes where the event occurred.	The organization being inspected/assessed configures the information system to generate audit records containing information that establishes where the event occurred For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 132.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed has configured the information system to generate audit records containing information that establishes where the event occurred. The organization conducting the inspection/assessment reviews the audit records generated to ensure that the records contain information that establishes where the event occurred. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 132.
AU-3	AU-3	CCI-000133	The information system generates audit records containing information that establishes the source of the event.	The organization being inspected/assessed configures the information system to generate audit records containing information that establishes the source of the event. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 133.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed has configured the information system to generate audit records containing information that establishes the source of the event. The organization conducting the inspection/assessment reviews the audit records generated to ensure that the records contain information that establishes the source of the event. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 133.
AU-3	AU-3	CCI-000134	The information system generates audit records containing information that establishes the outcome of the event.	The organization being inspected/assessed configures the information system to generate audit records containing information that establishes the outcome of the event. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 134.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed has configured the information system to generate audit records containing information that establishes the outcome of the event. The organization conducting the inspection/assessment reviews the audit records generated to ensure that the records contain information that establishes the outcome of the event. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 134.

AU-3	AU-3	CCI-001487	The information system generates audit records containing information that establishes the identity of any individuals or subjects associated with the event.	The organization being inspected/assessed configures the information system to generate audit records containing information that establishes the identity of any individuals or subjects associated with the event. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1487.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed has configured the information system to generate audit records containing information that establishes the identity of any individuals or subjects associated with the event. The organization conducting the inspection/assessment reviews the audit records generated to ensure that the records contain information that establishes the identity of any individuals or subjects associated with the event. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1487.
AU-3 (1)	AU-3 (1)	CCI-001488	The organization defines additional, more detailed information to be included in the audit records.	The organization being inspected/assessed defines and documents additional, more detailed information to be included in the audit records. The additional information must include at a minimum, full-text recording of privileged commands or the individual identities of group account users. The additional information must provide sufficient detail to reconstruct events to determine cause of compromise and magnitude of damage, malfunction, or security violation. DoD has determined that additional, more detailed information must include, at a minimum, full-text recording of privileged commands or the individual identities of group account users. DoD has determined that all additional, more detailed information is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented list of additional more detailed information to be included in the audit records to ensure that: 1. The list is defined; and 2. The list includes full-text recording of privileged commands or the individual identities of group account users. DoD has determined that additional, more detailed information must include, at a minimum, full-text recording of privileged commands or the individual identities of group account users. DoD has determined that it is not appropriate to define at the Enterprise level.
AU-3 (1)	AU-3 (1)	CCI-000135	The information system generates audit records containing the organization-defined additional, more detailed information that is to be included in the audit records.	The organization being inspected/assessed configures the information system to generate audit records containing the organization defined additional, more detailed information as defined in AU-3 (1), CCI 1488 that is to be included in the audit records. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 135.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed has configured the information system to generate audit records containing the organization defined additional, more detailed information as defined in AU-3 (1), CCI 1488 that is to be included in the audit records. The organization conducting the inspection/assessment reviews the audit records generated to ensure that the records contain organization defined additional, more detailed information that is to be included in the audit records. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 135.
AU-4	AU-4	CCI-001848	The organization defines the audit record storage requirements.	The organization being inspected/assessed defines and documents the required audit record storage capacity. DoD has determined the audit record storage requirements are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented audit record storage requirements to ensure the organization being inspected/assessed has defined those requirements. DoD has determined the audit record storage requirements are not appropriate to define at the Enterprise level.

AU-4	AU-4	CCI-001849	The organization allocates audit record storage capacity in accordance with organization-defined audit record storage requirements.	The organization being inspected/assessed allocates, and configures the information system to allocate audit record storage capacity as defined in AU-4, CCI 1848. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1849.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed has configured the information system to allocate audit record storage capacity as defined in AU-4, CCI 1848. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1849.
AU-4 (1)	AU-4 (1)	CCI-001851	The information system off-loads audit records per organization-defined frequency onto a different system or media than the system being audited.	The organization being inspected/assessed configures the information system to off-load audit records at a minimum, in real-time for interconnected systems and weekly for stand-alone systems onto a different system or media than the system being audited. DoD has defined the frequency as at a minimum, real-time for interconnected systems and weekly for stand-alone systems. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1851.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured the information system to off-load audit records at a minimum, in real-time for interconnected systems and weekly for stand-alone systems onto a different system or media than the system being audited. DoD has defined the frequency as at a minimum, real-time for interconnected systems and weekly for stand-alone systems. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1851.
AU-4 (1)	AU-4 (1)	CCI-001850	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.	DoD has defined the frequency as at a minimum, real-time for interconnected systems and weekly for stand-alone systems.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as at a minimum, real-time for interconnected systems and weekly for stand-alone systems.
AU-5	AU-5 (a)	CCI-000139	The information system alerts designated organization-defined personnel or roles in the event of an audit processing failure.	The organization being inspected/assessed configures the information system to alert at a minimum, the SCA and ISSO in the event of an audit processing failure. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 139. DoD has defined the personnel or roles as at a minimum, the SCA and ISSO.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured the information system to alert at a minimum, the SCA and ISSO in the event of an audit processing failure. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 139. DoD has defined the personnel or roles as at a minimum, the SCA and ISSO.
AU-5	AU-5 (a)	CCI-001572	The organization defines the personnel or roles to be alerted in the event of an audit processing failure.	The organization being inspected/assessed defines and documents any personnel or roles, in addition to the SCA and ISSO, who shall be alerted in the event of audit processing failure. If there are no additional personnel or roles, the organization must also document that. DoD has defined the personnel or roles as at a minimum, the SCA and ISSO.	The organization conducting the inspection/assessment obtains and examines the documented list of personnel or roles who should be alerted in the event of audit processing failure to ensure the organization being inspected/assessed has either defined additional personnel or roles, or identified that there are no additional personnel or roles. DoD has defined the personnel or roles as at a minimum, the SCA and ISSO.
AU-5	AU-5 (b)	CCI-000140	The information system takes organization defined actions upon audit failure (e.g., shut down information system, overwrite oldest audit records, stop generating audit records).	The organization being inspected/assessed configures the information system to take actions as defined in AU-5, CCI 1490 upon audit failure. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 140.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured the information system to take actions as defined in AU-5, CCI 1490 upon audit failure. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 140.

AU-5	AU-5 (b)	CCI-001490	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).	The organization being inspected/assessed will define and document actions to be taken by the information system upon audit failure. The organization shall consider trade-offs between the needs for system availability and audit integrity when defining the actions. Unless availability is an overriding concern, the default action should be to shut down the information system. DoD has determined that the actions are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented actions to ensure the organization being inspected/assessed has defined the actions to be taken by the information system upon audit failure. DoD has determined that the actions are not appropriate to define at the Enterprise level.
AU-5 (1)	AU-5 (1)	CCI-001852	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.	The organization being inspected/assessed defines and documents any personnel or roles, in addition to the ISSO/PMO and ISSM, who shall receive a warning when allocated audit record storage volume reaches a defined percentage of maximum audit records storage capacity. If there are no additional personnel or roles, the organization must also document that. DoD has defined the personnel or roles as at a minimum, the ISSO/PMO and ISSM.	The organization conducting the inspection/assessment obtains and examines the documented list of personnel or roles who should receive a warning when allocated audit record storage volume reaches a defined percentage of maximum audit records storage capacity to ensure the organization being inspected/assessed has either defined additional personnel or roles, or identified that there are no additional personnel or roles beyond the ISSO/PMO and ISSM. DoD has defined the personnel or roles as at a minimum, the ISSO/PMO and ISSM.
AU-5 (1)	AU-5 (1)	CCI-001853	The organization defines the time period within which organization-defined personnel, roles and/or location are to receive warnings when allocated audit record storage volume reaches a organization-defined percentage of maximum audit records storage capacity.	DoD has defined the time period as immediate.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as immediate.
AU-5 (1)	AU-5 (1)	CCI-001854	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.	DoD has defined the percentage as 75 percent.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the percentage as 75 percent.
AU-5 (1)	AU-5 (1)	CCI-001855	The information system provides a warning to organization-defined personnel, roles, and/or locations within organization-defined time period when allocated audit record storage volume reaches organization-defined percentage of repository maximum audit record storage capacity.	The organization being inspected/assessed configures the information system to immediately provide a warning to personnel, roles, and/or locations defined in AU-5 (1), CCI 1852 when allocated audit record storage volume reaches 75 percent of repository maximum audit record storage capacity. DoD has defined the time period as immediate. DoD has defined the percentage as 75 percent. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1855.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured the information system to immediately provide a warning to personnel, roles, and/or locations defined in AU-5 (1), CCI 1852 when allocated audit record storage volume reaches 75 percent of repository maximum audit record storage capacity. DoD has defined the time period as immediate. DoD has defined the percentage as 75 percent. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1855.
AU-6	AU-6 (a)	CCI-000148	The organization reviews and analyzes information system audit records on an organization defined frequency for indications of organization-defined inappropriate or unusual activity.	The organization being inspected/assessed documents and implements a process to review and analyze information system audit records every seven days or more frequently if required by an alarm event or anomaly for indications of activity defined in AU-6, CCI 1862. The organization must maintain an audit trail of the reviews. DoD has defined the frequency as every seven days or more frequently if required by an alarm event or anomaly.	The organization conducting the inspection/assessment obtains and examines the documented process for audit trail reviews as well as the audit trail showing the reviews to ensure the organization being inspected/assessed reviews and analyzes information system audit records every seven days or more frequently if required by an alarm event or anomaly for indications of activity defined in AU-6, CCI 1862. DoD has defined the frequency as every seven days or more frequently if required by an alarm event or anomaly.
AU-6	AU-6 (a)	CCI-000151	The organization defines the frequency for the review and analysis of information system audit records for organization-defined inappropriate or unusual activity.	DoD has defined the frequency as every seven days or more frequently if required by an alarm event or anomaly.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every seven days or more frequently if required by an alarm event or anomaly.

AU-6	AU-6 (a)	CCI-001862	The organization defines the types of inappropriate or unusual activity to be reviewed and analyzed in the audit records.	The organization being inspected/assessed defines and documents the types of inappropriate or unusual activity to be reviewed and analyzed in the audit records. DoD has determined that the types of inappropriate or unusual activity are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented types of inappropriate or unusual activity to ensure they have been defined. DoD has determined that the types of inappropriate or unusual activity are not appropriate to define at the Enterprise level.
AU-6	AU-6 (b)	CCI-000149	The organization reports any findings to organization-defined personnel or roles for indications of organization-defined inappropriate or unusual activity.	The organization being inspected/assessed documents and implements a process for reporting any findings of inappropriate or unusual activity as defined in AU-6, CCI 1862 to at a minimum, the ISSO and ISSM. DoD has defined the personnel or roles as at a minimum, the ISSO and ISSM.	The organization conducting the inspection/assessment obtains and examines the documented process for reporting findings as well as a sampling of historical reports to ensure the organization being inspected/assessed reports any findings of inappropriate or unusual activity as defined in AU-6, CCI 1862 to at a minimum, the ISSO and ISSM. DoD has defined the personnel or roles as at a minimum, the ISSO and ISSM.
AU-6	AU-6 (b)	CCI-001863	The organization defines the personnel or roles to receive the reports of organization-defined inappropriate or unusual activity.	The organization being inspected/assessed defines and documents any personnel or roles, in addition to the ISSO and ISSM, who shall receive the reports of inappropriate or unusual activity defined in AU-6, CCI 1862. If there are no additional personnel or roles, the organization must also document that. DoD has defined the personnel or roles as at a minimum, the ISSO and ISSM.	The organization conducting the inspection/assessment obtains and examines the documented list of personnel or roles who should receive the reports of inappropriate or unusual activity defined in AU-6, CCI 1862 to ensure the organization being inspected/assessed has either defined additional personnel or roles, or identified that there are no additional personnel or roles.
AU-6 (1)	AU-6 (1)	CCI-001864	The organization employs automated mechanisms to integrate audit review and analysis to support organizational processes for investigation of response to suspicious activities.	The organization being inspected/assessed identifies and implements automated mechanisms to integrate audit review and analysis. The goal is to support organizational investigation of and response to suspicious activities.	The organization conducting the inspection/assessment obtains and examines documentation identifying automated mechanisms to integrate audit review and analysis to ensure such mechanisms have been identified. The organization conducting the inspection/assessment examines the identified automated mechanisms to ensure they have been implemented.
AU-6 (1)	AU-6 (1)	CCI-001865	The organization employs automated mechanisms to integrate reporting processes to support organizational investigation of and response to suspicious activities.	The organization being inspected/assessed identifies and implements automated mechanisms to integrate reporting processes (e.g., centralized log analysis tools). The goal is to support organizational investigation of and response to suspicious activities.	The organization conducting the inspection/assessment obtains and examines documentation identifying automated mechanisms to integrate reporting processes to ensure such mechanisms have been identified. The organization conducting the inspection/assessment examines the identified automated mechanisms to ensure they have been implemented.
AU-6 (3)	AU-6 (3)	CCI-000153	The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.	The organization being inspected/assessed documents and implements a process to analyze and correlate audit records across different repositories to gain organization-wide situational awareness. The organization must maintain a record of the analysis.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of analysis to ensure the organization being inspected/assessed analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.
AU-6 (4)	AU-6 (4)	CCI-000154	The information system provides the capability to centrally review and analyze audit records from multiple components within the system.	The organization being inspected/assessed configures the information system to provide a capability to centrally review and analyze audit records from multiple components within the system. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 154.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured the information system to provide a capability to centrally review and analyze audit records from multiple components within the system. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 154.
AU-6 (10)	AU-6 (10)	CCI-001872	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.	The organization being inspected/assessed documents and implements a process for adjusting the level of audit review within the information system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information (e.g., INFOCON).	The organization conducting the inspection/assessment obtains and examines the documented process and supporting records to ensure the organization being inspected/assessed adjusts the level of audit review within the information system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.

AU-6 (10)	AU-6 (10)	CCI-001874	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.	The organization being inspected/assessed documents and implements a process for adjusting 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 (e.g., INFOCON).	The organization conducting the inspection/assessment obtains and examines the documented process and supporting records to ensure the organization being inspected/assessed 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.
AU-8	AU-8 (a)	CCI-000159	The information system uses internal system clocks to generate time stamps for audit records.	The organization being inspected/assessed configures the information system to use internal system clocks to generate time stamps for audit records. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 159.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed has configured the information system to use internal system clocks to generate time stamps for audit records. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 159.
AU-8	AU-8 (b)	CCI-001888	The organization defines the granularity of time measurement for time stamps generated for audit records.	DoD has defined the granularity of time measurement as one second.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the granularity of time measurement as one second.
AU-8	AU-8 (b)	CCI-001889	The information system records time stamps for audit records that meets organization-defined granularity of time measurement.	The organization being inspected/assessed configures the information system to generate time in the time stamps for audit records that meets one second granularity of time measurement. DoD has defined the granularity of time measurement as one second. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1889.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed has configured the information system to generate time in the time stamps for audit records that meets one second granularity of time measurement. DoD has defined the granularity of time measurement as one second. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1889.
AU-8	AU-8 (b)	CCI-001890	The information system records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT).	The organization being inspected/assessed configures the information system to generate time stamps for audit records that contain time zones or time offsets that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1890.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed has configured the information system to generate time stamps for audit records that contain time zones or time offsets that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT). For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1890.
AU-8 (1)	AU-8 (1)	CCI-000161	The organization defines the frequency for the synchronization of internal information system clocks.	DoD has defined the frequency as every 24 hours for networked systems.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every 24 hours for networked systems.
AU-8 (1)	AU-8 (1)	CCI-001492	The organization defines an authoritative time source for the synchronization of internal information system clocks.	DoD has defined the authoritative time source as an authoritative time server which is synchronized with redundant United States Naval Observatory (USNO) time servers as designated for the appropriate DoD network (NIPRNet / SIPRNet) and/or the Global Positioning System (GPS).	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the authoritative time source as an authoritative time server which is synchronized with redundant United States Naval Observatory (USNO) time servers as designated for the appropriate DoD network (NIPRNet / SIPRNet) and/or the Global Positioning System (GPS).

AU-8 (1)	AU-8 (1)	CCI-001891	The information system compares internal information system clocks on an organization-defined frequency with an organization-defined authoritative time source.	The organization being inspected/assessed configures the information system to synchronize internal information system clocks every 24 hours for networked systems with an authoritative time server which is synchronized with redundant United States Naval Observatory (USNO) time servers as designated for the appropriate DoD network (NIPRNet / SIPRNet) and/or the Global Positioning System (GPS) when the time difference is greater than the difference defined in AU-8 (1), CCI 1892. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1891. DoD has defined the frequency as every 24 hours for networked systems. DoD has defined the authoritative time source as an authoritative time server which is synchronized with redundant United States Naval Observatory (USNO) time servers as designated for the	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed has configured the information system to synchronize internal information system clocks every 24 hours for networked systems with an authoritative time server which is synchronized with redundant United States Naval Observatory (USNO) time servers as designated for the appropriate DoD network (NIPRNet / SIPRNet) and/or the Global Positioning System (GPS) when the time difference is greater than the difference defined in AU-8 (1), CCI 1892. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1891. DoD has defined the frequency as every 24 hours for networked systems. DoD has defined the authoritative time source as an authoritative time server which is synchronized with redundant United States Naval Observatory (USNO) time servers as designated for the appropriate DoD
AU-8 (1)	AU-8 (1)	CCI-001892	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.	The organization being inspected/assessed defines and documents the time difference, which, when exceeded, will require the information system to synchronize the internal information system clocks. DoD has determined the time difference is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented time difference to ensure the organization being inspected/assessed defines the time difference which, when exceeded, will require the information system to synchronize the internal information system clocks. DoD has determined the time difference is not appropriate to define at the Enterprise level.
AU-8 (1)	AU-8 (1)	CCI-002046	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.	The organization being inspected/assessed configures the information system to synchronize the internal system clocks to the authoritative time source when the time difference is greater than the time period defined in AU-8 (1), CCI 1892. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2046.	The organization conducting the inspection/assessment examines the information system to ensure the system synchronizes the internal system clocks to the authoritative time source when the time difference is greater than the time period defined in AU-8 (1), CCI 1892. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2046.
AU-9	AU-9	CCI-000162	The information system protects audit information from unauthorized access.	The organization being inspected/assessed configures the information system to disallow unauthorized access to audit information. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 162.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed has configured the information system to disallow unauthorized access to audit information. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 162.
AU-9	AU-9	CCI-000163	The information system protects audit information from unauthorized modification.	The organization being inspected/assessed configures the information system to disallow unauthorized modification of audit information. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 163.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed has configured the information system to disallow unauthorized modification of audit information. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 163.

AU-9	AU-9	CCI-000164	The information system protects audit information from unauthorized deletion.	The organization being inspected/assessed configures the information system to disallow unauthorized deletion of audit information. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 164.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed has configured the information system to disallow unauthorized deletion of audit information. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 164.
AU-9	AU-9	CCI-001493	The information system protects audit tools from unauthorized access.	The organization being inspected/assessed configures the information system to disallow unauthorized access to audit tools. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1493.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed has configured the information system to disallow unauthorized access to audit tools. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1493.
AU-9	AU-9	CCI-001494	The information system protects audit tools from unauthorized modification.	The organization being inspected/assessed configures the information system to disallow unauthorized modification of audit tools. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1494.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed has configured the information system to disallow unauthorized modification of audit tools. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1494.
AU-9	AU-9	CCI-001495	The information system protects audit tools from unauthorized deletion.	The organization being inspected/assessed configures the information system to disallow unauthorized deletion of audit tools. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1495.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed has configured the information system to disallow unauthorized deletion of audit tools. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1495.
AU-9 (4)	AU-9 (4) (a)	CCI-001351	The organization authorizes access to management of audit functionality to only organization-defined subset of privileged users.	The organization being inspected/assessed authorizes access to the management of audit functionality to only the subset of privileged users defined in AU-9 (4), CCI 1894.	The organization conducting the inspection/assessment obtains and examines the documentation of access authorizations for the management of audit functionality to ensure only the subset of privileged users defined in AU-9 (4), CCI 1894 have been granted access authorization.
AU-9 (4)	AU-9 (4)	CCI-001894	The organization defines the subset of privileged users who will be authorized access to the management of audit functionality.	The organization being inspected/assessed defines and documents the subset of privileged users to be authorized access to the management of audit functionality. DoD has determined the subset of privileged users is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented subset of privileged users to be authorized access to the management of audit functionality, to ensure the organization being inspected/assessed defines and documents the subset of privileged users to be authorized access to the management of audit functionality. DoD has determined the subset of privileged users is not appropriate to define at the Enterprise level.
AU-11	AU-11	CCI-000167	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.	The organization being inspected/assessed will take action to ensure it retains audit records for 5 years for SAMI; otherwise for at least 1 year to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements. DoD has defined the time period as 5 years for SAMI; otherwise for at least 1 year.	The organization conducting the inspection/assessment reviews the information system audit records and any other relevant documents or records to ensure the organization being inspected/assessed retains its audit records for 5 years for SAMI; otherwise for at least 1 year. DoD has defined the time period as 5 years for SAMI; otherwise for at least 1 year.

AU-11	AU-11	CCI-000168	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.	DoD has defined the time period as 5 years for SAMI; otherwise for at least 1 year.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as 5 years for SAMI; otherwise for at least 1 year.
AU-11 (1)	AU-11 (1)	CCI-002044	The organization defines measures to be employed to ensure that long-term audit records generated by the information system can be retrieved.	The organization being inspected/assessed defines and documents measures to be employed to ensure that long-term audit records generated by the information system can be retrieved. DoD has determined that the measures are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented measures to ensure the organization being inspected/assessed defines measures to be employed to ensure that long-term audit records generated by the information system can be retrieved. DoD has determined that the measures are not appropriate to define at the Enterprise level.
AU-11 (1)	AU-11 (1)	CCI-002045	The organization employs organization-defined measures to ensure that long-term audit records generated by the information system can be retrieved.	The organization being inspected/assessed employs the measures defined in AU-11 (1), CCI 2044 to ensure that long-term audit records generated by the information system can be retrieved.	The organization conducting the inspection/assessment obtains and examines the documented measures to ensure the organization being inspected/assessed employs the measures defined in AU-11 (1), CCI 2044 to ensure that long-term audit records generated by the information system can be retrieved.
AU-12	AU-12 (a)	CCI-000169	The information system provides audit record generation capability for the auditable events defined in AU-2 a at organization defined information system components.	The organization being inspected/assessed acquires or designs all information system and network components that provide audit record generation capability for the auditable events defined in AU-2 a. DoD has defined the information system components as all information system and network components.	The organization conducting the inspection/assessment examines the information system to ensure that all information system and network components provide audit record generation capability for the auditable events defined in AU-2 a. DoD has defined the information system components as all information system and network components.
AU-12	AU-12 (a)	CCI-001459	The organization defines information system components that provide audit record generation capability.	DoD has defined the information system components as all information system and network components.	DoD has defined the information system components as all information system and network components.
AU-12	AU-12 (b)	CCI-000171	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.	The organization being inspected/assessed configures the information system to ensure that only the ISSM or individuals appointed by the ISSM select which auditable events are to be audited by specific components of the information system. DoD has defined the personnel or roles as the ISSM or individuals appointed by the ISSM.	The organization conducting the inspection/assessment examines a sampling of information system components and confirms that the individuals capable of selecting auditable events are the ISSM or individuals appointed by the ISSM. DoD has defined the personnel or roles as the ISSM or individuals appointed by the ISSM.
AU-12	AU-12 (b)	CCI-001910	The organization defines the personnel or roles allowed select which auditable events are to be audited by specific components of the information system.	DoD has defined the personnel or roles as the ISSM or individuals appointed by the ISSM.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as the ISSM or individuals appointed by the ISSM.
AU-12	AU-12 (c)	CCI-000172	The information system generates audit records for the events defined in AU-2 d with the content defined in AU-3.	The organization being inspected/assessed configures the information system to generate audit records for the events defined in AU-2 d with the content defined in AU-3. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 172.	The organization conducting the inspection/assessment examines the information system to ensure that the system generates audit records for the events defined in AU-2 d with the content defined in AU-3. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 172.
AU-12 (1)	AU-12 (1)	CCI-000174	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 organization defined level of tolerance for relationship between time stamps of individual records in the audit trail.	The organization being inspected/assessed configures the information system to compile audit records from information system components defined in AU-12 (1), CCI 1577 into a system-wide (logical or physical) audit trail that is time-correlated to within the level of tolerance defined in AU-12 (1), CCI-000173 for relationship between time stamps of individual records in the audit trail. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 174.	The organization conducting the inspection/assessment examines the information system to ensure the information system is configured to compile audit records from information system components defined in AU-12 (1), CCI 1577 into a system-wide (logical or physical) audit trail that is time-correlated to within the level of tolerance defined in AU-12 (1), CCI-000173 for relationship between time stamps of individual records in the audit trail. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 174.

AU-12 (1)	AU-12 (1)	CCI-001577	The organization defines the information system components from which audit records are to be compiled into the system-wide audit trail.	The organization being inspected/assessed will define and document the information system components from which audit records are to be compiled into the system-wide audit trail. The organization will periodically update this list to ensure it is current. DoD has determined the information system components are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the system-wide audit trail documentation to ensure the organization being inspected/assessed maintains a current list of information system components. DoD has determined the information system components are not appropriate to define at the Enterprise level.
AU-12 (1)	AU-12 (1)	CCI-000173	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.	The organization being inspected/assessed will define and document their level of tolerance for variation in the time stamps applied to the audit data generated by the organization's information systems. DoD has determined that the level of tolerance is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment reviews the organization's audit and accountability policy and procedures addressing audit record generation and retention; information system audit configuration settings and associated documentation; information system audit records; and any other relevant documents or records. The objective is to validate the organization has defined and documented its level of tolerance for variation in the time stamps applied to the audit data generated by the organization's information systems. DoD has determined that the level of tolerance is not appropriate to define at the Enterprise level.
AU-12 (3)	AU-12 (3)	CCI-001913	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.	The organization being inspected/assessed defines and documents the individuals or roles that are to be provided the capability to change the auditing to be performed based on the selectable event criteria defined in AU-12 (3), CCI 1911, within the time thresholds defined in AU-12 (3), CCI 1912. DoD has determined that the individuals or roles are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented individuals or roles to ensure the organization being inspected/assessed defines the individuals or roles that are to be provided the capability to change the auditing to be performed based on the selectable event criteria defined in AU-12 (3), CCI 1911, within the time thresholds defined in AU-12 (3), CCI 1912. DoD has determined that the individuals or roles are not appropriate to define at the Enterprise level.
AU-12 (3)	AU-12 (3)	CCI-002047	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.	The organization being inspected/assessed defines and documents the information system components on which the auditing that is to be performed can be changed by individuals or roles defined in AU-12 (3), CCI 1913. DoD has determined the information system components are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented information system components to ensure the organization being inspected/assessed has defined the information system components on which the auditing that is to be performed can be changed by the individuals or roles defined in AU-12 (3), CCI 1913. DoD has determined the information system components are not appropriate to define at the Enterprise level.
AU-12 (3)	AU-12 (3)	CCI-001911	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.	The organization being inspected/assessed defines and documents the selectable event criteria for which changed auditing is to be performed. DoD has determined the selectable event criteria is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented selectable event criteria to ensure the organization being inspected/assessed defines the selectable event criteria for which changed auditing is to be performed. DoD has determined the selectable event criteria is not appropriate to define at the Enterprise level.
AU-12 (3)	AU-12 (3)	CCI-001912	The organization defines the time thresholds for organizational-defined individuals or roles to change the auditing to be performed based on organization-defined selectable event criteria.	The organization being inspected/assessed defines and documents the time thresholds for individuals or roles to change the auditing to be performed on information system components based on selectable event criteria defined in AU-12 (3), CCI 1911 occurs. DoD has determined the time thresholds are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented time thresholds to ensure the organization being inspected/assessed defines the time thresholds for individuals or roles to change the auditing to be performed on information system components based on selectable event criteria defined in AU-12 (3), CCI 1911 occurs. DoD has determined the time thresholds are not appropriate to define at the Enterprise level.

AU-12 (3)	AU-12 (3)	CCI-001914	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.	The organization being inspected/assessed configures the information system to provide the capability for individuals or roles defined in AU-12 (3), CCI 1913 to change the auditing to be performed on information system components defined in AU-12 (3), CCI 2047 based on selectable event criteria defined in AU-12 (3), CCI 1911 within time thresholds defined in AU-12 (3), CCI 1912. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1914.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to provide the capability for individuals or roles defined in AU-12 (3), CCI 1913 to change the auditing to be performed on information system components defined in AU-12 (3), CCI 2047 based on selectable event criteria defined in AU-12 (3), CCI 1911 within time thresholds defined in AU-12 (3), CCI 1912. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1914.
AU-14	AU-14 (b)	CCI-001919	The information system provides the capability for authorized users to select a user session to capture/record or view/hear.	The organization being inspected/assessed configures the information system to provide the capability for authorized users to select a user session to capture/record or view/hear. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1919.	The organization conducting the inspection/assessments examines the information system to ensure the organization being inspected/assessed configures the information system to provide the capability for authorized users to select a user session to capture/record or view/hear. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1919.
AU-14 (1)	AU-14 (1)	CCI-001464	The information system initiates session audits at system start-up.	The organization being inspected/assessed configures the information system to initiate session audits at system start-up. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1464.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to initiate session audits at system start-up. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1464.
AU-14 (2)	AU-14 (2)	CCI-001462	The information system provides the capability for authorized users to capture/record and log content related to a user session.	The organization being inspected/assessed configures the information system to provide the capability for authorized users to capture/record and log content related to a user session. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1462.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to provide the capability for authorized users to capture/record and log content related to a user session. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1462.
AU-14 (3)	AU-14 (3)	CCI-001920	The information system provides the capability for authorized users to remotely view/hear all content related to an established user session in real time.	The organization being inspected/assessed configures the information system to provide the capability for authorized users to remotely view/hear all content related to an established user session in real time. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1920.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to provide the capability for authorized users to remotely view/hear all content related to an established user session in real time. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1920.
CA-1	CA-1 (a)	CCI-002061	The organization defines the personnel or roles to whom security assessment and authorization policy is to be disseminated.	DoD has defined the personnel or roles as all personnel. DoD disseminates DoDI 8510.01 organization-wide via the DoD Issuances website. http://www.dtic.mil/whs/directives/corres/ins1.html	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as all personnel.

CA-1	CA-1 (a)	CCI-002062	The organization defines the personnel or roles to whom the security assessment and authorization procedures are to be disseminated.	DoD has defined the personnel or roles as all personnel.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as all personnel.
CA-1	CA-1 (a) (1)	CCI-000239	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.	DoDI 8510.01 meets the DoD requirement for security assessment authorization policy and procedures. DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8510.01.	DoDI 8510.01 meets the DoD requirement for security assessment authorization policy and procedures. DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8510.01.
CA-1	CA-1 (a) (1)	CCI-000240	The organization disseminates to organization-defined personnel or roles a security assessment and authorization policy.	DoD disseminates DoDI 8510.01 organization-wide via the DoD Issuances website. http://www.dtic.mil/whs/directives/corres/ins1.html	DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8510.01.
CA-1	CA-1 (a) (2)	CCI-000242	The organization develops and documents procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls.	The organization being inspected/assessed develops and documents, IAW DoDI 850.01, procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls.	The organization conducting the inspection/assessment obtains and examines the procedures to ensure the organization being inspected/assessedd evelops and documents procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls IAW DoDI 8510.01
CA-1	CA-1 (a) (2)	CCI-000243	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.	The organization being inspected/assessed will require all personnel to register at the DTIC website to receive update notifications to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls. DoD has defined the personnel or roles as all personnel.	The organization conducting the inspection/assessment obtains and examines the AUP (Acceptable Use Policy), appointment orders, or written policy requiring that all personnel register at the DTIC website to receive update notifications. DoD has defined the personnel or roles as all personnel.
CA-1	CA-1 (b) (1)	CCI-000238	The organization defines the frequency to review and update the current security assessment and authorization policy.	DoD has defined the frequency as every 5 years.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every 5 years.
CA-1	CA-1 (b) (1)	CCI-000241	The organization reviews and updates the current security assessment and authorization policy in accordance with organization-defined frequency.	DoDI 8510.01 meets the DoD requirement for security assessment authorization policy and procedures. DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8510.01.	DoDI 8510.01 meets the DoD requirement for security assessment authorization policy and procedures. DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8510.01.
CA-1	CA-1 (b) (2)	CCI-000244	The organization reviews and updates the current security assessment and authorization procedures in accordance with organization-defined frequency.	The organization being inspected/assessed reviews and updates, IAW DoDI 8510.01, the current security assessment and authorization procedures annually. The organization must maintain an audit trail of review and update activity. DoD has defined the frequency as annually.	The organization conducting the inspection/assessment obtains and examines the audit trail of review and update activity to ensure the organization being inspected/assessed reviews and updates, IAW DoDI 8510.01, the current security assessment and authorization procedures annually.
CA-1	CA-1 (b) (2)	CCI-001578	The organization defines the frequency to review and update the current security assessment and authorization procedures.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.
CA-2	CA-2 (a)	CCI-000245	The organization develops a security assessment plan for the information system and its environment of operation. IG&VP WG Note: *For DoD, the security assessment plan information is included in the Security Plan and the security assessment report and is not a separate document/artifact.*	The organization being inspected/assessed will document these security assessment plan requirements as part of the DoD approved Security Plan. Security plan templates are provided through eMASS and the Knowledge Service. *Comment* The items required within this control are being split into the security plan and security assessment report to eliminate creation of an additional artifact.	The organization conducting the inspection/assessment obtains and examines the Security Plan to validate *security assessment blocks* are complete.

CA-2	CA-2 (a) (1)	CCI-000246	The organization's security assessment plan describes the security controls and control enhancements under assessment. IG&VP WG Note *For DoD, the security assessment plan information is included in the Security Plan and the security assessment report and is not a separate document/artifact.*	The organization being inspected/assessed will ensure the Security Plan identifies the security controls and control enhancements under assessment. *Comment* The items required within this control are being split into the security plan and security assessment report to eliminate creation of an additional artifact.	The organization conducting the inspection/assessment obtains the security assessment plan to verify the plan identifies the security controls and those control enhancements under assessment.
CA-2	CA-2 (a) (2)	CCI-000247	The organization's security assessment plan describes assessment procedures to be used to determine security control effectiveness. IG&VP WG Note: *For DoD, the security assessment plan information is included in the Security Plan and the security assessment report and is not a separate document/artifact.*	The implementation guidance and validation procedures posted on the Knowledge Service constitutes assessment procedures for DoD. If organizations being inspected/assessed use assessment procedures other than those posted on the Knowledge Service, those procedures must be documented. *Comment* The items required within this control are being split into the security plan and security assessment report to eliminate creation of an additional artifact.	DoD components are automatically compliant with this control if using the implementation guidance and validation procedures on the Knowledge Service. If the organization being inspected/assessed is using alternative implementation guidance and validation procedures, the organization conducting the inspection/assessment will obtain and examine those procedures.
CA-2	CA-2 (a) (3)	CCI-000248	The organization's security assessment plan describes assessment environment. *For DoD, the security assessment plan information is included in the Security Plan and the security assessment report and is not a separate document/artifact.*	The organization being inspected/assessed will provide a description of the authorization boundary in their Security Plan. Authorization boundary can be described via one or more of the following: network diagrams, data flow diagrams, system design documents, or a list of information system components. Authorization boundary as defined in CNSSI 4009. *Comment* The items required within this control are being split into the security plan and security assessment report to eliminate creation of an additional artifact.	The organization conducting the inspection/assessment obtains and examines the organization's authorization boundary. Authorization boundary can be described via one or more of the following: network diagrams, data flow diagrams, system design documents, or a list of information system components.
CA-2	CA-2 (a) (3)	CCI-002070	The organization's security assessment plan describes assessment team, assessment roles and responsibilities.	The organization being inspected/assessed lists their assessment team members and their associated assessment roles and responsibilities in the security assessment plan.	The organization conducting the inspection/assessment obtains and examines the security assessment plan to ensure the organization being inspected/assessed lists their assessment team members and their associated assessment roles and responsibilities in the security assessment plan.
CA-2	CA-2 (b)	CCI-000251	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. IG&VP WG Note: *For DoD, the security assessment plan information is included in the Security Plan and the security assessment report and is not a separate document/artifact.*	In accordance with DoD's published guidance, the organization being inspected/assessed will utilize the implementation guidance and validation procedures published on the Knowledge Service to evaluate the implementation status of the applicable controls. DoD has defined the frequency as annually for technical controls, annually for a portion of management and operational controls, such that all are reviewed in a 3 year period, except for those requiring more frequent review as defined in other site or overarching policy. (NOTE: Technical, Management and Operational is IAW NIST SP 800-53 Table 1-1). *Comment* The items required within this control are being split into the security plan and security assessment report to eliminate creation of an additional artifact.	See CA-2 c "The organization conducting the inspection/assessment obtains and examines the security assessment report to verify that it includes the compliance/non-compliance status of all controls and specific deficiencies for all non-compliant controls."

CA-2	CA-2 (b)	CCI-000252	The organization defines the frequency on which the security controls in the information system and its environment of operation are assessed. IG&VP WG Note: *For DoD, the security assessment plan information is included in the Security Plan and the security assessment report and is not a separate document/artifact.*	DoD has defined the frequency as annually for technical controls, annually for a portion of management and operation controls such that all are reviewed in a 3 year period except for those requiring more frequent review as defined in other site or overarching policy. NOTE: Technical, Management and Operational is IAW NIST SP 800-53 Table 1-1. *Comment* The items required within this control are being split into the security plan and security assessment report to eliminate creation of an additional artifact.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually for technical controls, annually for a portion of management and operation controls such that all are reviewed in a 3 year period except for those requiring more frequent review as defined in other site or overarching policy. NOTE: Technical, Management and Operational is IAW NIST SP 800-53 Table 1-1.
CA-2	CA-2 (c)	CCI-000253	The organization produces a security assessment report that documents the results of the assessment against the information system and its environment of operation. IG&VP WG Note: *For DoD, the security assessment plan information is included in the Security Plan and the security assessment report and is not a separate document/artifact.*	The organization being inspected/assessed will develop a SAR that includes the compliance/non-compliance status of all controls and specific deficiencies for all non-compliant controls using the template available on the Knowledge Service. *Comment* The items required within this control are being split into the security plan and security assessment report to eliminate creation of an additional artifact.	The organization conducting the inspection/assessment obtains and examines the SAR to verify that it includes the compliance/non-compliance status of all controls and specific deficiencies for all non-compliant controls.
CA-2	CA-2 (d)	CCI-000254	The organization provides the results of the security control assessment against information system and its environment of operation to organization-defined individuals or roles. IG&VP WG Note: *For DoD, the security assessment plan information is included in the Security Plan and the security assessment report and is not a separate document/artifact.*	The organization being inspected/assessed will provide the SAR to at a minimum, the ISSO and ISSM. DoD has defined the individuals or roles as at a minimum, the ISSO and ISSM. *Comment* The items required within this control are being split into the security plan and security assessment report to eliminate creation of an additional artifact.	The organization conducting the inspection/assessment interviews at a minimum, the ISSO and ISSM to ensure the SAR has been received. DoD has defined the individuals or roles as at a minimum, the ISSO and ISSM.
CA-2	CA-2 (d)	CCI-002071	The organization defines the individuals or roles to whom the results of the security control assessment is to be provided.	DoD has defined the individuals or roles as at a minimum, the ISSO and ISSM.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the individuals or roles as at a minimum, the ISSO and ISSM.
CA-2 (1)	CA-2 (1)	CCI-000255	The organization employs assessors or assessment teams with organization-defined level of independence to conduct security control assessments of organizational information systems.	The organization being inspected/assessed will employ assessors and assessor teams with the level of independence defined in CA-2 (1), CCI 2064 to conduct security control assessments of organizational information systems.	The organization conducting the inspection/assessment obtains and examines the level of independence defined in CA-2 (1), CCI 2064 to ensure that they, as the assessor, meet the required level of independence.
CA-2 (1)	CA-2 (1)	CCI-002063	The organization defines the level of independence for assessors or assessment teams to conduct security control assessments of organizational information systems.	The organization being inspected/assessed defines and documents the level of independence for assessors or assessment teams to conduct security control assessments of organizational information systems. DoD has determined the level of independence is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented level of independence to ensure the organization being inspected/assessed defines the level of independence for assessors or assessment teams to conduct security control assessments of organizational information systems. DoD has determined the level of independence is not appropriate to define at the Enterprise level.
CA-3	CA-3 (a)	CCI-000257	The organization authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements.	The organization being inspected/assessed will develop and certify, by appropriate signatures (e.g. AO, network managers), Interconnection Security Agreements (e.g., MOU, MOA, SLA) authorizing the connection of its information systems to other information systems. Policy Note: Interconnection security agreements are required for systems connecting between enclaves that require the hosting enclave to enable PPS outside of their already established and approved business practices. Connections can include both DoD enclaves or non DoD enclaves.	The organization conducting the inspection/assessment obtains and examines documentation of the Interconnection Security Agreements to include appropriate signatures. Policy Note: Interconnection security agreements are required for systems connecting between enclaves that require the hosting enclave to enable PPS outside of their already established and approved business practices. Connections can include both DoD enclaves or non DoD enclaves.

CA-3	CA-3 (b)	CCI-000258	The organization documents, for each interconnection, the interface characteristics.	The organization being inspected/assessed will document the interface characteristics for each interconnection. Use of external reporting databases for these characteristics when tied to the specific interconnection is acceptable (e.g., ports, protocols, and services). Policy Note: Interconnection security agreements are required for systems connecting between enclaves that require the hosting enclave to enable PPS outside of their already established and approved business practices. Connections can include both DoD enclaves or non DoD enclaves.	The organization conducting the inspection/assessment obtains and examines interconnection security agreement documentation. Policy Note: Interconnection security agreements are required for systems connecting between enclaves that require the hosting enclave to enable PPS outside of their already established and approved business practices. Connections can include both DoD enclaves or non DoD enclaves.
CA-3	CA-3 (b)	CCI-000259	The organization documents, for each interconnection, the security requirements.	The organization being inspected/assessed will, for each interconnection, identify and document any additional security controls to be implemented to protect the confidentiality, integrity, and availability of the connected systems and the data passing between them. Controls should be appropriate for the systems to be connected and the environment in which the interconnection will operate. Policy Note: Interconnection security agreements are required for systems connecting between enclaves that require the hosting enclave to enable PPS outside of their already established and approved business practices. Connections can include both DoD enclaves or non DoD enclaves.	The organization conducting the inspection/assessment obtains and examines interconnection security agreement documentation, specifically looking at any additional security controls identified for implementation. Policy Note: Interconnection security agreements are required for systems connecting between enclaves that require the hosting enclave to enable PPS outside of their already established and approved business practices. Connections can include both DoD enclaves or non DoD enclaves.
CA-3	CA-3 (b)	CCI-000260	The organization documents, for each interconnection, the nature of the information communicated.	The organization being inspected/assessed will document in the interconnection security agreement the type of information being transferred/transmitted. Characteristics will include but are not limited to: classification, information type (e.g. PII, HIPAA, FOUO, financial data, etc.) Policy Note: Interconnection security agreements are required for systems connecting between enclaves that require the hosting enclave to enable PPS outside of their already established and approved business practices. Connections can include both DoD enclaves or non DoD enclaves.	The organization conducting the inspection/assessment obtains and examines the interconnection security agreement documentation, specifically to identify the type of information being transferred/transmitted. Characteristics will include but are not limited to: classification, information type (e.g. PII, HIPAA, FOUO, financial data, etc.) Policy Note: Interconnection security agreements are required for systems connecting between enclaves that require the hosting enclave to enable PPS outside of their already established and approved business practices. Connections can include both DoD enclaves or non DoD enclaves.
CA-3	CA-3 (c)	CCI-002083	The organization reviews and updates Interconnection Security Agreements on an organization-defined frequency.	The organization being inspected/assessed reviews and updates Interconnection Security Agreements at least annually. The organization must maintain an audit trail of reviews and updates. DoD has defined the frequency as at least annually.	The organization conducting the inspection/assessment obtains and examines the audit trail of reviews and updates to ensure the organization being inspected/assessed reviews and updates Interconnection Security Agreements at least annually. DoD has defined the frequency as at least annually.
CA-3	CA-3 (c)	CCI-002084	The organization defines the frequency that reviews and updates to the Interconnection Security Agreements must be conducted.	DoD has defined the frequency as at least annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as at least annually.
CA-3 (1)	CA-3 (1)	CCI-002072	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.	DoD has defined the unclassified, national security systems as all unclassified NSS.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the unclassified, national security systems as all unclassified NSS.
CA-3 (1)	CA-3 (1)	CCI-002073	The organization defines the boundary protection device to be used to connect organization-defined unclassified, national security systems to an external network.	The organization being inspected/assessed defines and documents the boundary protection device to be used to connect organization-defined unclassified, national security systems to an external network. DoD has determined the boundary protection device is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented boundary protection device to ensure the organization being inspected/assessed defines the boundary protection device to be used to connect organization-defined unclassified, national security systems to an external network. DoD has determined the boundary protection device is not appropriate to define at the Enterprise level.

CA-3 (1)	CA-3 (1)	CCI-000262	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.	The organization being inspected/assessed documents in its policy and procedures addressing information system connections, the organization will prohibit DoD has defined the unclassified, national security systems as all unclassified NSS from having a direct connection to an external network without the use of a boundary protection device defined in CA-3 (1), CCI 262. DoD has defined the unclassified, national security systems as all unclassified NSS.	The organization conducting the inspection/assessment obtains and examines policy document prohibiting direct connection of all unclassified NSS to external networks without the use of a boundary protection device defined in CA-3 (1), CCI 262. DoD has defined the unclassified, national security systems as all unclassified NSS.
CA-3 (5)	CA-3 (5)	CCI-002081	The organization defines the information systems that employ either allow-all, deny-by-exception or deny-all, permit by exception policy for allowing connection to external information systems.	DoD has defined the information systems as any systems requiring external connectivity.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the information systems as any systems requiring external connectivity.
CA-3 (5)	CA-3 (5)	CCI-002082	The organization selects either allow-all, deny-by exception or deny-all, permit by exception policy for allowing organization-defined information systems to connect to external information systems.	The organization being inspected/assessed selects deny-all, permit by exception policy for allowing any systems requiring external connectivity to connect to external information systems. DoD has defined the information systems as any systems requiring external connectivity.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed selects deny-all, permit by exception policy for allowing any systems requiring external connectivity to connect to external information systems. DoD has defined the information systems as any systems requiring external connectivity.
CA-3 (5)	CA-3 (5)	CCI-002080	The organization employs either an allow-all, deny-by exception or deny-all, permit by exception policy for allowing organization-defined information systems to connect to external information systems.	The organization being inspected/assessed configures the information system to employ a deny-all, permit by exception policy for allowing any systems requiring external connectivity to connect to external information systems. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2080. DoD has defined the information systems as any systems requiring external connectivity.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to employ a deny-all, permit by exception policy for allowing any systems requiring external connectivity to connect to external information systems. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2080. DoD has defined the information systems as any systems requiring external connectivity.
CA-5	CA-5 (a)	CCI-000264	The organization develops a plan of action and milestones for the information system to document the organizations 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.	The organization being inspected/assessed will develop a security POA&M in accordance with DoDI 8510.01 Enclosure 6. POA&M templates are available on the Knowledge Service.	The organization conducting the inspection/assessment obtains and examines the security POA&M for compliance with DoDI 8510.01.
CA-5	CA-5 (b)	CCI-000265	The organization defines the frequency to update existing plan of action and milestones for the information system.	DoD has defined the frequency as at least every 90 days.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as at least every 90 days.
CA-5	CA-5 (b)	CCI-000266	The organization updates, on an organization-defined frequency, existing plan of action and milestones based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.	The organization being inspected/assessed will update the POA&M at least every 90 days. The updates are to be based upon the assessment of the identified vulnerabilities and weaknesses, prioritization of the vulnerabilities and weaknesses, progress being made in addressing and resolving the security weaknesses and vulnerabilities found in programs and systems, and continuous monitoring activities. DoD has defined the frequency as at least every 90 days.	The organization conducting the inspection/assessment obtains and examines current POA&M. The objective is to validate the organization is providing updates to the POA&M at least every 90 days. Review of POA&M without change must be documented (i.e., adding review date to the POA&M header information). DoD has defined the frequency as at least every 90 days.
CA-6	CA-6 (a)	CCI-000270	The organization assigns a senior-level executive or manager as the authorizing official for the information system.	The organization being inspected/assessed will assign a senior-level executive or manager as the official role, and the responsibility, for authorizing the information system(s). Assignment must be in writing and IAW with DoDI 8510.01 (i.e. Appointment memorandum).	The organization conducting the inspection/assessment obtains and examines the written appointment memorandum.

CA-6	CA-6 (b)	CCI-000271	The organization ensures the authorizing official authorizes the information system for processing before commencing operations.	The organization being inspected/assessed will ensure that an authorization document (e.g. authorization to operate (ATO), interim authorization to operate (IATO)) has been issued by the authorizing official (AO) prior to placing the information system into an operational status.	The organization conducting the inspection/assessment obtains and examines the authorization document to ensure the information system is authorized prior to being placed into operational status.
CA-6	CA-6 (c)	CCI-000273	The organization defines the frequency of updating the security authorization.	DoD has defined the frequency as at least every three years, whenever there is a significant change to the system, or if there is a change to the environment in which the system operates.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as at least every three years, whenever there is a significant change to the system, or if there is a change to the environment in which the system operates.
CA-6	CA-6 (c)	CCI-000272	The organization updates the security authorization on an organization-defined frequency.	The organization being inspected/assessed updates the security authorization at least every three years, whenever there is a significant change to the system, or if there is a change to the environment in which the system operates. DoD has defined the frequency as at least every three years, whenever there is a significant change to the system, or if there is a change to the environment in which the system operates.	The organization conducting the inspection/assessment obtains and examines the security authorization documentation to confirm the security authorization has been updated within the last three years, when there was a significant change to the system, or if there was a change to the environment in which the system operates. DoD has defined the frequency as at least every three years, whenever there is a significant change to the system, or if there is a change to the environment in which the system operates.
CA-7	CA-7	CCI-000274	The organization develops a continuous monitoring strategy.	Future DoD-wide CM guidance to be published	Future DoD-wide CM guidance to be published
CA-7	CA-7 (a)	CCI-002087	The organization establishes and defines the metrics to be monitored for the continuous monitoring program.	Future DoD-wide CM guidance to be published	Future DoD-wide CM guidance to be published
CA-7	CA-7 (b)	CCI-002088	The organization establishes and defines the frequencies for continuous monitoring.	Future DoD-wide CM guidance to be published	Future DoD-wide CM guidance to be published
CA-7	CA-7 (b)	CCI-002089	The organization establishes and defines the frequencies for assessments supporting continuous monitoring.	Future DoD-wide CM guidance to be published	Future DoD-wide CM guidance to be published
CA-7	CA-7 (c)	CCI-000279	The organization implements a continuous monitoring program that includes ongoing security control assessments in accordance with the organizational continuous monitoring strategy.	Future DoD-wide CM guidance to be published	Future DoD-wide CM guidance to be published
CA-7	CA-7 (d)	CCI-002090	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.	Future DoD-wide CM guidance to be published	Future DoD-wide CM guidance to be published
CA-7	CA-7 (e)	CCI-002091	The organization implements a continuous monitoring program that includes correlation and analysis of security-related information generated by assessments and monitoring.	Future DoD-wide CM guidance to be published	Future DoD-wide CM guidance to be published
CA-7	CA-7 (f)	CCI-002092	The organization implements a continuous monitoring program that includes response actions to address results of the analysis of security-related information.	Future DoD-wide CM guidance to be published	Future DoD-wide CM guidance to be published
CA-7	CA-7 (g)	CCI-000281	The organization defines the frequency to report the security status of organization and the information system to organization-defined personnel or roles.	Future DoD-wide CM guidance to be published	Future DoD-wide CM guidance to be published
CA-7	CA-7 (g)	CCI-001581	The organization defines personnel or roles to whom the security status of organization and the information system should be reported.	Future DoD-wide CM guidance to be published	Future DoD-wide CM guidance to be published
CA-7	CA-7 (g)	CCI-000280	The organization implements a continuous monitoring program that includes reporting the security status of organization and the information system to organization-defined personnel or roles on an organization-defined frequency.	Future DoD-wide CM guidance to be published	Future DoD-wide CM guidance to be published
CA-9	CA-9 (a)	CCI-002101	The organization authorizes internal connections of organization-defined information system components or classes of components to the information system.	The organization being inspected/assessed authorizes internal connections of information system components defined in CA-9, CCI 2102 or classes of components to the information system. The organization must maintain an audit trail of authorizations.	The organization conducting the inspection/assessment obtains and examines the audit trail of authorizations to ensure the organization being inspected/assessed authorizes internal connections of information system components defined in CA-9, CCI 2102 or classes of components to the information system.

CA-9	CA-9 (a)	CCI-002102	The organization defines the information system components or classes of components that that are authorized internal connections to the information system.	The organization being inspected/assessed defines and documents the information system components or classes of components that that are authorized internal connections to the information system. DoD has determined the information system components are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented information system components to ensure the organization being inspected/assessed defines the information system components or classes of components that that are authorized internal connections to the information system. DoD has determined the information system components are not appropriate to define at the Enterprise level.
CA-9	CA-9 (b)	CCI-002103	The organization documents, for each internal connection, the interface characteristics.	The organization being inspected/assessed documents, for each internal connection, the interface characteristics.	The organization conducting the inspection/assessment obtains and examines the documented interface characteristics as well as the network topology to ensure the organization being inspected/assessed documents, for each internal connection, the interface characteristics.
CA-9	CA-9 (b)	CCI-002104	The organization documents, for each internal connection, the security requirements.	The organization being inspected/assessed documents, for each internal connection, the security requirements.	The organization conducting the inspection/assessment obtains and examines the documented security requirements as well as the network topology to ensure the organization being inspected/assessed documents, for each internal connection, the security requirements.
CA-9	CA-9 (b)	CCI-002105	The organization documents, for each internal connection, the nature of the information communicated.	The organization being inspected/assessed documents, for each internal connection, the nature of the information communicated.	The organization conducting the inspection/assessment obtains and examines the documented nature of information communication as well as the network topology to ensure the organization being inspected/assessed documents, for each internal connection, the nature of the information communicated.
CM-1	CM-1 (a)	CCI-001821	The organization defines the organizational personnel or roles to whom the configuration management policy is to be disseminated.	DoD has defined the organizational personnel or roles as all stakeholders in the configuration management process.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the organizational personnel or roles as all stakeholders in the configuration management process.
CM-1	CM-1 (a)	CCI-001824	The organization defines the organizational personnel or roles to whom the configuration management procedures are to be disseminated.	DoD has defined the organizational personnel or roles as all stakeholders in the configuration management process.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the organizational personnel or roles as all stakeholders in the configuration management process.
CM-1	CM-1 (a) (1)	CCI-000287	The organization develops and documents a configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	The organization being inspected/assessed develops and documents a configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	The organization conducting the inspection/assessment obtains and examines the configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
CM-1	CM-1 (a) (1)	CCI-001822	The organization disseminates the configuration management policy to organization defined personnel or roles.	The organization being inspected/assessed disseminates a configuration management policy via an information sharing capability (e.g. portal, intranet, email, etc.) to all stakeholders in the configuration management process. DoD has defined the organizational personnel or roles as all stakeholders in the configuration management process.	The organization conducting the inspection/assessment obtains and examines the configuration management policy via the inspected organization's information sharing capability (e.g. portal, intranet, email, etc.) to ensure it has been disseminated.
CM-1	CM-1 (a) (2)	CCI-000290	The organization develops and documents procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.	The organization being inspected/assessed develops and documents procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.	The organization conducting the inspection/assessment obtains and examines the procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.
CM-1	CM-1 (a) (2)	CCI-001825	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.	The organization being inspected/assessed disseminates the procedures to facilitate the implementation of the configuration management policy and associated configuration management controls via an information sharing capability (e.g. portal, intranet, email, etc.) to all stakeholders in the configuration management process. DoD has defined the organizational personnel or roles as all stakeholders in the configuration management process.	The organization conducting the inspection/assessment obtains and examines the procedures to facilitate the implementation of the configuration management policy and associated configuration management controls via the inspected organization's information sharing capability (e.g. portal, intranet, email, etc.) to ensure it has been disseminated.

CM-1	CM-1 (b) (1)	CCI-000289	The organization reviews and updates, on an organization defined frequency, the configuration management policy.	The organization being inspected/assessed reviews and updates, annually, the configuration management policy. The organization must document each occurrence of the reviews and update actions as an audit trail. DoD has defined the frequency as annually.	The organization conducting the inspection/assessment obtains and examines documentation of occurrence of reviews and update actions for the configuration management policy to ensure annual review and necessary updates are occurring. DoD has defined the frequency as annually.
CM-1	CM-1 (b) (1)	CCI-000286	The organization defines a frequency to review and update the configuration management policies.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.
CM-1	CM-1 (b) (2)	CCI-000292	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.	The organization being inspected/assessed reviews and updates, annually, the procedures to facilitate the implementation of the configuration management policy and associated configuration management controls. The organization must document each occurrence of the reviews and update actions as an audit trail. DoD has defined the frequency as annually.	The organization conducting the inspection/assessment obtains and examines documentation of occurrence of reviews and update actions for the procedures to facilitate the implementation of the configuration management policy and associated configuration management controls to ensure annual review and necessary updates are occurring. DoD has defined the frequency as annually.
CM-1	CM-1 (b) (2)	CCI-001584	The organization defines the frequency to review and update configuration management procedures.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.
CM-2	CM-2	CCI-000293	The organization develops and documents a current baseline configuration of the information system.	The organization being inspected/assessed develops and documents a current baseline configuration of the information system.	The organization conducting the inspection/assessment obtains and examines the documented baseline configuration.
CM-2	CM-2	CCI-000295	The organization maintains under configuration control, a current baseline configuration of the information system.	The organization being inspected/assessed maintains a current baseline configuration of the information system.	The organization conducting the inspection/assessment obtains and examines the current baseline to ensure the current configuration matches the current documented baseline.
CM-2 (1)	CM-2 (1) (a)	CCI-000296	The organization reviews and updates the baseline configuration of the information system at an organization-defined frequency.	The organization being inspected/assessed reviews and updates the baseline configuration of the information system annually. The organization must document each occurrence of the reviews and update actions as an audit trail. DoD has defined the frequency as annually.	The organization conducting the inspection/assessment obtains and examines documentation of organizational reviews and update actions for the baseline configuration to ensure annual review and necessary updates are occurring. DoD has defined the frequency as annually.
CM-2 (1)	CM-2 (1) (a)	CCI-001497	The organization defines a frequency for the reviews and updates to the baseline configuration of the information system.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.
CM-2 (1)	CM-2 (1) (b)	CCI-000297	The organization reviews and updates the baseline configuration of the information system when required due to organization-defined circumstances.	The organization being inspected/assessed reviews and updates the baseline configuration of the information system when required due to baseline configuration changes or as events dictate such as changes due to USCYBERCOM tactical orders/ directives or cyber attacks. The organization must document each occurrence of the reviews and update actions as an audit trail. DoD has defined the circumstances as baseline configuration changes or as events dictate such as changes due to USCYBERCOM tactical orders/ directives or cyber attacks.	The organization conducting the inspection/assessment obtains and examines documentation of organizational reviews and update actions for the baseline configuration of the information system when required due to baseline configuration changes or as events dictate such as changes due to USCYBERCOM tactical orders/ directives or cyber attacks to ensure review and necessary updates are occurring. DoD has defined the circumstances as baseline configuration changes or as events dictate such as changes due to USCYBERCOM tactical orders/ directives or cyber attacks.
CM-2 (1)	CM-2 (1) (b)	CCI-001585	The organization defines the circumstances that require reviews and updates to the baseline configuration of the information system.	DoD has defined the circumstances as baseline configuration changes or as events dictate such as changes due to USCYBERCOM tactical orders/ directives or cyber attacks.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the circumstances as baseline configuration changes or as events dictate such as changes due to USCYBERCOM tactical orders/ directives or cyber attacks.

CM-2 (1)	CM-2 (1) (c)	CCI-000298	The organization reviews and updates the baseline configuration of the information system as an integral part of information system component installations.	The organization being inspected/assessed reviews and updates the baseline configuration of the information system as an integral part of information system component installations. The organization must document each occurrence of the reviews and update actions as an audit trail.	The organization conducting the inspection/assessment obtains and examines documentation of organizational reviews and update actions for the baseline configuration of the information system as an integral part of information system component installations to ensure review and necessary updates are occurring.
CM-2 (1)	CM-2 (1) (c)	CCI-000299	The organization reviews and updates the baseline configuration of the information system as an integral part of information system component upgrades.	The organization being inspected/assessed reviews and updates the baseline configuration of the information system as an integral part of information system component upgrades. The organization must document each occurrence of the reviews and update actions as an audit trail.	The organization conducting the inspection/assessment obtains and examines documentation of organizational reviews and update actions for the baseline configuration of the information system as an integral part of information system component upgrades to ensure review and necessary updates are occurring.
CM-3	CM-3 (a)	CCI-000313	The organization determines the types of changes to the information system that are configuration controlled.	The organization being inspected/assessed determines the types of changes to the information system that are to be configuration controlled. This action will be implemented by the CCB as defined in CM-3, CCI 1586.	The organization conducting the inspection/assessment obtains and examines the configuration management policy and plan to ensure the organization identifies the types of changes to the information system that are configuration controlled.
CM-3	CM-3 (b)	CCI-001740	The organization reviews proposed configuration controlled changes to the information system.	The organization being inspected/assessed conducts reviews of records documenting the proposed configuration controlled changes to each information system. The organization will maintain an audit trail of each proposed configuration controlled change. This action will be implemented by the CCB as defined in CM-3, CCI 1586.	The organization conducting the inspection/assessment obtains and examines the audit trail of a sampling of proposed configuration controlled changes to ensure the reviews are being conducted.
CM-3	CM-3 (b)	CCI-000314	The organization approves or disapproves configuration controlled changes to the information system with explicit consideration for security impact analysis.	The organization being inspected/assessed approves or disapproves configuration controlled changes to the information system with explicit consideration for security impact analysis. The organization must maintain an audit trail of approval/disapproval of configuration controlled changes. This action will be implemented by the CCB as defined in CM-3, CCI 1586.	The organization conducting the inspection/assessment obtains and examines the audit trail of the approval/disapproval of configuration controlled changes to ensure a security impact analysis was conducted.
CM-3	CM-3 (c)	CCI-001741	The organization documents configuration change decisions associated with the information system.	The organization being inspected/assessed documents configuration change decisions associated with the information system. The organization must maintain an audit trail of configuration change decisions. This action will be implemented by the CCB as defined in CM-3, CCI 1586.	The organization conducting the inspection/assessment obtains and examines the audit trail documenting configuration change decisions associated with the information system to ensure the organization being inspected/assessed has documented their decisions.
CM-3	CM-3 (d)	CCI-001819	The organization implements approved configuration-controlled changes to the information system.	The organization being inspected/assessed implements approved configuration-controlled changes to the information system. The organization must maintain an audit trail of the implementation of approved configuration-controlled changes.	The organization conducting the inspection/assessment obtains and examines the audit trail documenting the implementation of approved configuration-controlled changes to the information system to ensure the organization being inspected/assessed has implemented the approved changes.
CM-3	CM-3 (e)	CCI-000316	The organization retains records of configuration-controlled changes to the information system for an organization-defined time period.	The organization being inspected/assessed retains records of all configuration-controlled changes to the information system, as a result of CM-3, CCI 1819, for a time period defined by the organization's CCB. DoD has defined the time period as a time period defined by the organization's CCB.	The organization conducting the inspection/assessment obtains and examines the records of all configuration-controlled changes to the information system to ensure the organization being inspected/assessed retains the records of all configuration controlled changes for a time period defined by the organization's CCB. DoD has defined the time period as a time period defined by the organization's CCB.
CM-3	CM-3 (e)	CCI-002056	The organization defines the time period the record of configuration-controlled changes are to be retained.	DoD has defined the time period as a time period defined by the organization's CCB.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as a time period defined by the organization's CCB.

CM-3	CM-3 (f)	CCI-000318	The organization audits and reviews activities associated with configuration controlled changes to the system.	The organization being inspected/assessed audits and reviews activities associated with configuration-controlled changes to the information system. The organization must maintain an audit trail to include review activities associated with configuration-controlled changes.	The organization conducting the inspection/assessment obtains and examines the audit trail documenting the review activities associated with configuration-controlled changes to the information system to ensure the organization being inspected/assessed audits and reviews activities associated with the changes.
CM-3	CM-3 (g)	CCI-000319	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.	The organization being inspected/assessed coordinates and provides oversight for configuration change control activities through a configuration control board (CCB) that convenes at a frequency determined by the CCB and/or for any configuration change conditions determined by the CCB. DoD has defined the configuration change control element as a configuration control board. DoD has defined the frequency as at a frequency determined by the CCB. DoD has defined the configuration change conditions as configuration change conditions determined by the CCB.	The organization conducting the inspection/assessment obtains and examines the organization's configuration management policy and plan; document/charter establishing the organization's CCB; meeting minutes; information system change control records; and any other relevant documents or records. The objective of the review is to validate the organization is coordinating and overseeing the configuration change control activities through a CCB.
CM-3	CM-3 (g)	CCI-000320	The organization defines frequency to convene configuration change control element.	The organization being inspected/assessed defines within their CCB Charter, the frequency for configuration change control review. DoD has defined the frequency as at a frequency determined by the CCB.	The organization conducting the inspection/assessment obtains and examines the CCB Charter to ensure the frequency for configuration change control review is defined. DoD has defined the frequency as at a frequency determined by the CCB.
CM-3	CM-3 (g)	CCI-000321	The organization defines configuration change conditions that prompt the configuration change control element to convene.	The organization being inspected/assessed defines within their CCB Charter, the configuration change conditions that prompt the configuration change control element to convene. DoD has defined the configuration change conditions as configuration change conditions determined by the CCB.	The organization conducting the inspection/assessment obtains and examines the CCB Charter to ensure the configuration change conditions that prompt the configuration change control element to convene are defined. DoD has defined the configuration change conditions as configuration change conditions determined by the CCB.
CM-3	CM-3 (g)	CCI-001586	The organization defines the configuration change control element (e.g., committee, board) responsible for coordinating and providing oversight for configuration change control activities.	DoD has defined the configuration change control element as a configuration control board (CCB).	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the configuration change control element as a configuration control board (CCB).
CM-3 (4)	CM-3 (4)	CCI-000332	The organization requires an information security representative to be a member of the organization-defined configuration change control element.	The organization being inspected/assessed requires an information security representative to be a member of the configuration control board. DoD has defined the configuration change control element as the configuration control board.	The organization conducting the inspection/assessment obtains and examines the membership list of the organization's configuration control board to ensure an information security representative is a member of the organization's configuration control board.
CM-3 (6)	CM-3 (6)	CCI-001745	The organization defines the security safeguards that are to be provided by the cryptographic mechanisms which are employed by the organization.	DoD has defined the security safeguards as all security safeguards.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the security safeguards as all security safeguards.
CM-3 (6)	CM-3 (6)	CCI-001746	The organization ensures that cryptographic mechanisms used to provide organization-defined security safeguards are under configuration management.	The organization being inspected/assessed ensures that cryptographic mechanisms used to provide all security safeguards are under configuration management. DoD has defined the security safeguards as all security safeguards.	The organization conducting the inspection/assessment obtains and examines the configuration management policy to ensure that cryptographic mechanisms used to provide all security safeguards are documented in the policy. DoD has defined the security safeguards as all security safeguards.
CM-4	CM-4	CCI-000333	The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.	The organization being inspected/assessed analyzes changes to the information system to determine potential security impacts prior to change implementation. The organization must maintain records of analysis of changes to the information system.	The organization conducting the inspection/assessment obtains and examines the records of analyses to ensure the organization is conducting a security impact analysis of changes to the information system(s) prior to their implementation.
CM-5	CM-5	CCI-000338	The organization defines physical access restrictions associated with changes to the information system.	The organization being inspected/assessed defines and documents in the configuration management policy, physical access restrictions associated with changes to the information system.	The organization conducting the inspection/assessment obtains and examines the configuration management policy to ensure the organization being inspected/assessed defines physical access restrictions associated with changes to the information system.

CM-5	CM-5	CCI-000339	The organization documents physical access restrictions associated with changes to the information system.	The organization being inspected/assessed documents, in the configuration management policy, physical access restrictions associated with changes to the information system.	The organization conducting the inspection/assessment obtains and examines the configuration management policy to ensure the organization being inspected/assessed documents physical access restrictions associated with changes to the information system.
CM-5	CM-5	CCI-000340	The organization approves physical access restrictions associated with changes to the information system.	The organization being inspected/assessed documents and implements a process to approve physical access restrictions associated with changes to the information system. The organization must maintain an audit trail of approvals.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of approvals to ensure the organization being inspected/assessed approves physical access restrictions associated with changes to the information system.
CM-5	CM-5	CCI-000341	The organization enforces physical access restrictions associated with changes to the information system.	The organization being inspected/assessed documents and implements a process to enforce physical access restrictions associated with changes to the information system.	The organization conducting the inspection/assessment the documented process to ensure the organization being inspected/assessed enforces physical access restrictions associated with changes to the information system as documented in the configuration management policy.
CM-5	CM-5	CCI-000342	The organization defines logical access restrictions associated with changes to the information system.	The organization being inspected/assessed defines and documents in the configuration management policy, logical access restrictions associated with changes to the information system.	The organization conducting the inspection/assessment obtains and examines the configuration management policy to ensure the organization being inspected/assessed defines logical access restrictions associated with changes to the information system.
CM-5	CM-5	CCI-000343	The organization documents logical access restrictions associated with changes to the information system.	The organization being inspected/assessed documents, in the configuration management policy, logical access restrictions associated with changes to the information system.	The organization conducting the inspection/assessment obtains and examines the configuration management policy to ensure the organization being inspected/assessed documents logical access restrictions associated with changes to the information system.
CM-5	CM-5	CCI-000344	The organization approves logical access restrictions associated with changes to the information system.	The organization being inspected/assessed documents and implements a process to approve logical access restrictions associated with changes to the information system. The organization must maintain an audit trail of approvals.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of approvals to ensure the organization being inspected/assessed approves logical access restrictions associated with changes to the information system.
CM-5	CM-5	CCI-000345	The organization enforces logical access restrictions associated with changes to the information system.	The organization being inspected/assessed documents and implements a process to enforce logical access restrictions associated with changes to the information system. The information system must maintain an audit trail of logical access to the information system pertaining to information system changes.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the logical access audit trail to ensure the organization being inspected/assessed enforces logical access restrictions associated with changes to the information system as documented in the configuration management policy.
CM-5 (5)	CM-5 (5) (a)	CCI-001753	The organization limits privileges to change information system components within a production or operational environment.	The organization being inspected/assessed documents and implements a process to limit privileges to change information system components within a production or operational environment.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed limits privileges to change information system components within a production or operational environment.
CM-5 (5)	CM-5 (5) (a)	CCI-001754	The organization limits privileges to change system-related information within a production or operational environment.	The organization being inspected/assessed documents and implements a process to limit privileges to change system-related information within a production or operational environment.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed limits privileges to change system-related information within a production or operational environment.
CM-5 (5)	CM-5 (5) (b)	CCI-001827	The organization defines frequency to review information system privileges.	DoD has defined the frequency as every 90 days.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every 90 days.
CM-5 (5)	CM-5 (5) (b)	CCI-001828	The organization defines frequency to reevaluate information system privileges.	DoD has defined the frequency as every 90 days.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every 90 days.
CM-5 (5)	CM-5 (5) (b)	CCI-001829	The organization reviews information system privileges per organization defined frequency.	The organization being inspected/assessed reviews information system privileges every 90 days. The organization must maintain the reviews as an audit trail. DoD has defined the frequency as every 90 days.	The organization conducting the inspection/assessment obtains and examines the audit trail of reviews to ensure the organization being inspected/assessed reviews information system privileges every 90 days . DoD has defined the frequency as every 90 days.

CM-5 (5)	CM-5 (5) (b)	CCI-001830	The organization reevaluates information system privileges per organization defined frequency.	The organization being inspected/assessed reevaluates information system privileges every 90 days . The organization must maintain the reevaluations as an audit trail. DoD has defined the frequency as every 90 days.	The organization conducting the inspection/assessment obtains and examines the audit trail of reviews to ensure the organization being inspected/assessed reevaluates information system privileges every 90 days. DoD has defined the frequency as every 90 days.
CM-5 (6)	CM-5 (6)	CCI-001499	The organization limits privileges to change software resident within software libraries.	The organization being inspected/assessed documents and implements a process to limit privileges to accounts authorized to change software resident within software libraries. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1499.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed limits privileges to change software resident within software libraries. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1499.
CM-6	CM-6 (a)	CCI-000363	The organization defines security configuration checklists to be used to establish and document configuration settings for the information system technology products employed.	DoD has defined the security configuration checklists as DoD security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.). The organization being inspected/assessed documents in the security plan, the configuration guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.) which apply to their information system components.	DoD has defined the security configuration checklists as DoD security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.). The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed has documented the configuration guidance which apply to their information system components. The organization conducting the inspection/assessment reviews the list of documented guidance to ensure that all applicable guidance is identified given the information system components within the authorization boundary.
CM-6	CM-6 (a)	CCI-000364	The organization establishes configuration settings for information technology products employed within the information system using organization-defined security configuration checklists.	DoD security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.) meet the DoD requirement for establishing configuration settings. DoD Components are automatically compliant with this control because they are covered by the DoD level security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.).	DoD security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.) meet the DoD requirement for establishing configuration settings. DoD Components are automatically compliant with this control because they are covered by the DoD level security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.).
CM-6	CM-6 (a)	CCI-000365	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.	DoD security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.) meet the DoD requirement for documenting configuration settings. DoD Components are automatically compliant with this control because they are covered by the DoD level security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.).	DoD security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.) meet the DoD requirement for documenting configuration settings. DoD Components are automatically compliant with this control because they are covered by the DoD level security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.).
CM-6	CM-6 (a)	CCI-001588	The organization-defined security configuration checklists reflect the most restrictive mode consistent with operational requirements.	DoD security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.) meet the DoD requirement for ensuring security configuration checklists reflect the most restrictive mode consistent with operational requirements. DoD Components are automatically compliant with this control because they are covered by the DoD level security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.).	DoD security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.) meet the DoD requirement for ensuring security configuration checklists reflect the most restrictive mode consistent with operational requirements. DoD Components are automatically compliant with this control because they are covered by the DoD level security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.).

CM-6	CM-6 (b)	CCI-000366	The organization implements the security configuration settings.	The organization being inspected/assessed must develop and document a process for implementing DoD security configuration or implementation guidance (e.g. STIGs, NSA configuration guides, CTOs, DTMs etc.). DoD has defined the security configuration checklists as DoD security configuration or implementation guidance (e.g. STIGs, NSA configuration guides, CTOs, DTMs etc.).	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed implements DoD security configuration or implementation guidance (e.g. STIGs, NSA configuration guides, CTOs, DTMs etc.). The organization conducting the inspection/assessment tests a sampling of information system components to ensure they comply with the required settings. DoD has defined the security configuration checklists as DoD security configuration or implementation guidance (e.g. STIGs, NSA configuration guides, CTOs, DTMs etc.).
CM-6	CM-6 (c)	CCI-000367	The organization identifies any deviations from the established configuration settings for organization-defined information system components based on organization-defined operational requirements.	The organization being inspected/assessed documents in the security plan and POA&M, if applicable, the information system components as defined in CM-6, CCI 1755 which deviate from configuration settings, and which settings as defined in CM-6, CCI 1756.	The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed has documented deviations from configuration settings for information system components.
CM-6	CM-6 (c)	CCI-000368	The organization documents any deviations from the established configuration settings for organization-defined information system components based on organization-defined operational requirements.	The organization being inspected/assessed documents in the security plan and POA&M, if applicable, all configurable information system components which deviate from configuration settings, and which settings as defined in CM-6, CCI 1756. DoD has defined the information system components as all configurable information system components.	The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed has documented deviations from configuration settings for information system components.
CM-6	CM-6 (c)	CCI-000369	The organization approves any deviations from the established configuration settings for organization-defined information system components based on organization-defined operational requirements.	The organization being inspected/assessed manages and approves changes to the security plan documenting deviations IAW CM-3, CCI 314. The organization must maintain an audit trail of approved changes to the security plan.	The organization conducting the inspection/assessment obtains and examines the security plan and the audit trail of approved changes to ensure the deviations are approved IAW CM-3, CCI 314.
CM-6	CM-6 (c)	CCI-001755	The organization defines the information system components for which any deviation from the established configuration settings are to be identified, documented and approved.	DoD has defined the information system components as all configurable information system components.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the information system components as all configurable information system components.
CM-6	CM-6 (c)	CCI-001756	The organization defines the operational requirements on which the configuration settings for the organization-defined information system components are to be based.	The organization being inspected/assessed must define and document in the system security plan, the requirements which may deviate from the approved configuration settings on the information system components defined in CM-6, CCI 1755. DoD has determined that it is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the system security plan to ensure the organization being inspected/assessed defines the requirements which may deviate from the approved configuration settings on the information system components defined in CM-6, CCI 1755. DoD has determined that it is not appropriate to define at the Enterprise level.
CM-6	CM-6 (d)	CCI-001502	The organization monitors changes to the configuration settings in accordance with organizational policies and procedures.	The organization being inspected/assessed develops and documents a process for monitoring changes to the configuration settings in accordance with organizational policies and procedures.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed monitors changes to the configuration settings in accordance with organizational policies and procedures.
CM-6	CM-6 (d)	CCI-001503	The organization controls changes to the configuration settings in accordance with organizational policies and procedures.	The organization being inspected/assessed develops and documents a process for controlling changes to the configuration settings in accordance with organizational policies and procedures.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed controls changes to the configuration settings in accordance with organizational policies and procedures.
CM-7	CM-7 (b)	CCI-000380	The organization defines for the information system prohibited or restricted functions, ports, protocols, and/or services.	DoD has defined the information system prohibited or restricted functions, ports, protocols, and/or services as IAW DoDI 8551.01.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the information system prohibited or restricted functions, ports, protocols, and/or services as IAW DoDI 8551.01.
CM-7	CM-7 (a)	CCI-000381	The organization configures the information system to provide only essential capabilities.	The organization being inspected/assessed documents in the security plan, essential capabilities which the information system must provide. The organization being inspected/assessed configures the information system to provide only those documented essential capabilities.	The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed has identified essential capabilities. The organization conducting the inspection/assessment inspects the information system to ensure that it provides only those documented essential capabilities.

CM-7	CM-7 (b)	CCI-000382	The organization configures the information system to prohibit or restrict the use of organization-defined functions, ports, protocols, and/or services.	The organization being inspected/assessed configures the information system to prohibit or restrict the use of functions, ports, protocols, and/or services IAW DoDI 8551.01. DoD has defined the information system prohibited or restricted functions, ports, protocols, and/or services as IAW DoDI 8551.01.	The organization conducting the inspection/assessment inspects the information system to ensure the organization being inspected/assessed prohibits or restricts the use of functions, ports, protocols, and/or services IAW DoDI 8551.01. DoD has defined the information system prohibited or restricted functions, ports, protocols, and/or services as IAW DoDI 8551.01.
CM-7 (1)	CM-7 (1) (a)	CCI-000384	The organization reviews the information system per organization defined frequency to identify unnecessary and nonsecure functions, ports, protocols, and services.	The organization being inspected/assessed documents and implements a process to review the information system every 30 days to identify unnecessary and nonsecure functions, ports, protocols, and services. The organization must maintain an audit trail of the reviews. DoD has defined the frequency as every 30 days.	The organization conducting the inspection/assessment obtains and examines the documented process and audit trail of reviews to ensure the organization being inspected/assessed reviews the information system every 30 days to identify unnecessary and nonsecure functions, ports, protocols, and services. DoD has defined the frequency as every 30 days.
CM-7 (1)	CM-7 (1) (a)	CCI-001760	The organization defines the frequency of information system reviews to identify unnecessary and/or nonsecure functions, ports, protocols, and services.	DoD has defined the frequency as every 30 days.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every 30 days.
CM-7 (1)	CM-7 (1) (b)	CCI-001761	The organization defines the functions, ports, protocols and services within the information system that are to be disabled when deemed unnecessary and/or nonsecure.	The organization being inspected/assessed must define and document in the system security plan, the functions, ports, protocols and services within the information system that are to be disabled when deemed unnecessary. DoD has determined that it is not appropriate to define unnecessary functions, ports, protocols and service at the Enterprise level. Nonsecure functions, ports, protocols and services are defined in DoDI 8551.01.	The organization conducting the inspection/assessment obtains and examines the system security plan to ensure the organization being inspected/assessed defines the functions, ports, protocols and services within the information system that are to be disabled when deemed unnecessary. DoD has determined that it is not appropriate to define unnecessary functions, ports, protocols and service at the Enterprise level. Nonsecure functions, ports, protocols and services are defined in DoDI 8551.01.
CM-7 (1)	CM-7 (1) (b)	CCI-001762	The organization disables organization-defined functions, ports, protocols, and services within the information system deemed to be unnecessary and/or nonsecure.	The organization being inspected/assessed must disable functions, ports, protocols, and services within the information system deemed to be unnecessary and/or nonsecure as defined in CM-7 (1), CCI 1761.	The organization conducting the inspection/assessment inspects the information system to ensure the organization being inspected/assessed disables functions, ports, protocols, and services within the information system deemed to be unnecessary and/or nonsecure as defined in CM-7 (1), CCI 1761.
CM-7 (2)	CM-7 (2)	CCI-001592	The organization defines the rules authorizing the terms and conditions of software program usage on the information system.	The organization being inspected/assessed defines and documents their rules for approval of software program usage. For network capable software programs, the organization being inspected/assessed complies with DoDI 8551. DoD has determined that the rules authorizing the terms and conditions of software program usage on the information system are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the rules as well as the software list to ensure that all network capable software programs are DoDI 8551 compliant and that the rules authorizing the use of all other programs are defined. DoD has determined that the rules authorizing the terms and conditions of software program usage on the information system are not appropriate to define at the Enterprise level
CM-7 (2)	CM-7 (2)	CCI-001763	The organization defines the policies regarding software program usage and restrictions.	The organization being inspected/assessed defines and documents their rules for approval of software program usage. For network capable software programs, the organization being inspected/assessed complies with DoDI 8551. DoD has determined that the rules authorizing the terms and conditions of software program usage on the information system are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the rules as well as the software list to ensure that all network capable software programs are DoDI 8551 compliant and that the rules authorizing the use of all other programs are defined. DoD has determined that the rules authorizing the terms and conditions of software program usage on the information system are not appropriate to define at the Enterprise level.
CM-7 (2)	CM-7 (2)	CCI-001764	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.	The organization being inspected/assessed configures the information system to prevent the execution of programs not authorized in accordance with CM-7 (2) CCIs 1592 and 1763.	The organization conducting the inspection/assessment examines the information systems to ensure the systems are configured to prevent the execution of programs not authorized in accordance with CM-7 (2) CCIs 1592 and 1763.
CM-7 (3)	CM-7 (3)	CCI-000387	The organization defines registration requirements for functions, ports, protocols, and services.	DoD has defined the registration requirements as IAW DoDI 8551.01.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the registration requirements as IAW DoDI 8551.01.

CM-7 (3)	CM-7 (3)	CCI-000388	The organization ensures compliance with organization-defined registration requirements for functions, ports, protocols, and services.	The organization being inspected/assessed implements DoDI 8551.01. DoD has defined the registration requirements as IAW DoDI 8551.01.	The organization conducting the inspection/assessment obtains and examines a documented listing of ports, protocols, and services in use, and reviews a sampling of those ports, protocols, and services to ensure the organization being inspected/assessed is compliant with DoDI 8551.01. DoD has defined the registration requirements as IAW DoDI 8551.01.
CM-7 (5)	CM-7 (5) a	CCI-001772	The organization defines the software programs authorized to execute on the information system.	The organization being inspected/assessed must define and document software programs that are authorized to execute on the information system. DoD has determined that a comprehensive list of unauthorized software programs is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented list of software programs that are authorized to execute to ensure that list is defined. DoD has determined that a comprehensive list of unauthorized software programs is not appropriate to define at the Enterprise level.
CM-7 (5)	CM-7 (5) a	CCI-001773	The organization identifies the organization-defined software programs authorized to execute on the information system.	The organization being inspected/assessed must define and document software programs that are authorized to execute on the information system.	The organization conducting the inspection/assessment obtains and examines the documented list of software programs that are authorized to execute to ensure that list is defined.
CM-7 (5)	CM-7 (5) b	CCI-001774	The organization employs an deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system.	The organization being inspected/assessed configures the information system to deny-all and only permit by exception the execution of authorized software programs on the information system.	The organization conducting the inspection/assessment examines the information system to ensure that it is configured to deny-all and only permit by exception the execution of authorized software programs on the information system.
CM-7 (5)	CM-7 (5) c	CCI-001775	The organization defines the frequency on which it will review and update the list of authorized software programs.	DoD has defined the frequency as monthly.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as monthly.
CM-7 (5)	CM-7 (5) c	CCI-001777	The organization reviews and updates the list of authorized software programs per organization-defined frequency.	The organization being inspected/assessed documents and implements a process to review and update the list of authorized software programs monthly. The organization must maintain an audit trail of the review and update activity. DoD has defined the frequency as monthly.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of reviews and updates to ensure that the organization being inspected/assessed reviews and updates the list of authorized software programs monthly. DoD has defined the frequency as monthly.
CM-8	CM-8 (a) (1)	CCI-000389	The organization develops and documents an inventory of information system components that accurately reflects the current information system.	The organization being inspected/assessed documents inventory of information system components that accurately reflects the current information system.	The organization conducting the inspection/assessment obtains and examines the documented inventory and examines a sampling of information system components to ensure inventory accurately reflects the current information system.
CM-8	CM-8 (a) (2)	CCI-000392	The organization develops and documents an inventory of information system components that includes all components within the authorization boundary of the information system.	The organization being inspected/assessed documents inventory of information system components that includes all components within the authorization boundary of the information system.	The organization conducting the inspection/assessment obtains and examines the documented inventory and examines a sampling of information system components to ensure inventory includes all components within the authorization boundary of the information system.
CM-8	CM-8 (a) (3)	CCI-000395	The organization develops and documents an inventory of information system components that is at the level of granularity deemed necessary for tracking and reporting.	The organization being inspected/assessed documents inventory of information system components that is at the level of granularity deemed necessary for tracking and reporting.	The organization conducting the inspection/assessment obtains and examines the documented inventory and examines a sampling of information system components to ensure inventory is at the level of granularity deemed necessary for tracking and reporting.
CM-8	CM-8 (a) (4)	CCI-000398	The organization defines information deemed necessary to achieve effective information system component accountability.	DoD has defined the information as hardware inventory specifications (manufacturer, type, model, serial number, physical location), software license information, information system/component owner, and for a networked component/device, the machine name.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the information as hardware inventory specifications (manufacturer, type, model, serial number, physical location), software license information, information system/component owner, and for a networked component/device, the machine name.
CM-8	CM-8 (a) (4)	CCI-000399	The organization develops and documents an inventory of information system components that includes organization defined information deemed necessary to achieve effective information system component accountability.	The organization being inspected/assessed documents inventory of information system components that includes organization defined information deemed necessary to achieve effective information system component accountability.	The organization conducting the inspection/assessment obtains and examines the documented inventory and examines a sampling of information system components to ensure inventory includes organization defined information deemed necessary to achieve effective information system component accountability.
CM-8	CM-8 (b)	CCI-001779	The organization defines the frequency on which the information system component inventory is to be reviewed and updated	DoD has defined the frequency as at a minimum, annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as at a minimum, annually.

CM-8	CM-8 (b)	CCI-001780	The organization reviews and updates the information system component inventory per organization-defined frequency.	The organization being inspected/assessed documents and implements a process to review and update the information system component inventory at a minimum, annually. The organization must maintain an audit trail of review and update activity. DoD has defined the frequency as at a minimum, annually.	The organization conducting the inspection/assessment obtains and examines the documented process for reviews and updates as well as the audit trail of reviews and updates to ensure the organization being inspected/assessed reviews and updates the information system component inventory at a minimum, annually. DoD has defined the frequency as at a minimum, annually.
CM-8 (2)	CM-8 (2)	CCI-000411	The organization employs automated mechanisms to help maintain an up-to-date inventory of information system components.	The organization being inspected/assessed documents and implements automated mechanisms to help maintain an up-to-date inventory of information system components. An automated mechanism implemented IAW CM-2 (2) satisfies the requirements of this CCI if the automated mechanism maintains an up-to-date inventory.	The organization conducting the inspection/assessment obtains and examines the documentation identifying the automated mechanism used to help maintain an up-to-date inventory of information system components and examines the mechanism to ensure the organization being inspected/assessed employs automated mechanisms to help maintain an up-to-date inventory of information system components.
CM-8 (2)	CM-8 (2)	CCI-000412	The organization employs automated mechanisms to help maintain a complete inventory of information system components.	The organization being inspected/assessed documents and implements automated mechanisms to help maintain a complete inventory of information system components. An automated mechanism implemented IAW CM-2 (2) satisfies the requirements of this CCI if the automated mechanism maintains a complete inventory.	The organization conducting the inspection/assessment obtains and examines the documentation identifying the automated mechanism used to help maintain a complete inventory of information system components and examines the mechanism to ensure the organization being inspected/assessed employs automated mechanisms to help maintain a complete inventory of information system components.
CM-8 (2)	CM-8 (2)	CCI-000413	The organization employs automated mechanisms to help maintain a accurate inventory of information system components.	The organization being inspected/assessed documents and implements automated mechanisms to help maintain an accurate inventory of information system components. An automated mechanism implemented IAW CM-2 (2) satisfies the requirements of this CCI if the automated mechanism maintains an accurate inventory.	The organization conducting the inspection/assessment obtains and examines the documentation identifying the automated mechanism used to help maintain an accurate inventory of information system components and examines the mechanism to ensure the organization being inspected/assessed employs automated mechanisms to help maintain an accurate inventory of information system components.
CM-8 (2)	CM-8 (2)	CCI-000414	The organization employs automated mechanisms to help maintain a readily available inventory of information system components.	The organization being inspected/assessed documents and implements automated mechanisms to help maintain a readily available inventory of information system components. An automated mechanism implemented IAW CM-2 (2) satisfies the requirements of this CCI if the automated mechanism maintains a readily available inventory.	The organization conducting the inspection/assessment obtains and examines the documentation identifying the automated mechanism used to help maintain a readily available inventory of information system components and examines the mechanism to ensure the organization being inspected/assessed employs automated mechanisms to help maintain a readily available inventory of information system components.
CM-8 (3)	CM-8 (3) (a)	CCI-000415	The organization defines the frequency of employing automated mechanism to detect the presence of unauthorized hardware, software, and firmware components within the information system.	DoD has defined the frequency as continuously.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as continuously.
CM-8 (3)	CM-8 (3) (a)	CCI-000416	The organization employs automated mechanisms, per organization defined frequency, to detect the presence of unauthorized hardware, software, and firmware components within the information system.	The organization being inspected/assessed documents and implements automated mechanisms to detect the presence of unauthorized hardware, software, and firmware components within the information system continuously. DoD has defined the frequency as continuously.	The organization conducting the inspection/assessment obtains and examines the documentation identifying the automated mechanisms and examines the implemented automated mechanisms to ensure the organization being inspected/assessed employs automated mechanisms, continuously, to detect the presence of unauthorized hardware, software, and firmware components within the information system. DoD has defined the frequency as continuously.
CM-8 (3)	CM-8 (3) (b)	CCI-001783	The organization defines the personnel or roles to be notified when unauthorized hardware, software, and firmware components are detected within the information system.	The organization being inspected/assessed defines and documents any personnel or roles, in addition to the ISSO or ISSM, to be notified when unauthorized hardware, software, and firmware components are detected within the information system. If there are no additional personnel or roles, the organization must also document that. DoD has defined the personnel or roles as the ISSO and ISSM and others as the local organization deems appropriate.	The organization conducting the inspection/assessment obtains and examines the documented list of personnel or roles to be notified when unauthorized hardware, software, and firmware components are detected within the information system to ensure the organization being inspected/assessed has either defined additional personnel or roles, or identified that there are no additional personnel or roles. DoD has defined the personnel or roles as the ISSO and ISSM and others as the local organization deems appropriate.

CM-8 (3)	CM-8 (3) (b)	CCI-001784	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.	The organization being inspected/assessed documents and implements a process to take action to disable network access by unauthorized software, hardware, and firmware components, isolate the components, and/or notify the ISSO and ISSM and others as the local organization deems appropriate. The organization must maintain an audit trail of actions taken upon detection of unauthorized software, hardware, and firmware components. DoD has defined the personnel or roles as the ISSO and ISSM and others as the local organization deems appropriate.	The organization conducting the inspection/assessment obtains and examines the documented process and audit trail for taking action upon detection of unauthorized components to ensure the organization being inspected/assessed takes action to disable network access by unauthorized software, hardware, and firmware components, isolate the components, and/or notify the ISSO and ISSM and others as the local organization deems appropriate. DoD has defined the personnel or roles as the ISSO and ISSM and others as the local organization deems appropriate.
CM-9	CM-9 (a)	CCI-000421	The organization develops and documents a configuration management plan for the information system that addresses roles, responsibilities, and configuration management processes and procedures.	The organization being inspected/assessed will develop and document a configuration management plan for the information system that addresses roles, responsibilities, and configuration management processes and procedures.	The organization conducting the inspection/assessment obtains and examines the configuration management plan to verify that it addresses and documents roles, responsibilities, and configuration management processes and procedures
CM-9	CM-9 (a)	CCI-000423	The organization implements a configuration management plan for the information system that addresses roles, responsibilities, and configuration management processes and procedures.	The organization being inspected/assessed will implement a configuration management plan for the information system that addresses roles, responsibilities, and configuration management processes and procedures.	The organization conducting the inspection/assessment obtains and examines the configuration management plan as well as evidence of implementation (e.g., completed change requests, meeting minutes, and other relevant documents) to ensure the organization being inspected/assessed implements a configuration management plan for the information system that addresses roles, responsibilities, and configuration management processes and procedures.
CM-9	CM-9(c)	CCI-000424	The organization develops and documents a configuration management plan for the information system that defines the configuration items for the information system.	The organization being inspected/assessed will develop and document a configuration management plan for the information system that defines the configuration items.	The organization conducting the inspection/assessment obtains and examines the configuration management plan to ensure it defines and documents the configuration items for the information system.
CM-9	CM-9 (c)	CCI-000426	The organization implements a configuration management plan for the information system that defines the configuration items for the information system.	The organization being inspected/assessed will implement a configuration management plan for the information system that defines the configuration items.	The organization conducting the inspection/assessment obtains and examines the configuration management plan to ensure the organization being inspected/assessed implements a configuration management plan for the information system that defines the configuration items.
CM-9	CM-9 (b)	CCI-001790	The organization develops and documents a configuration management plan for the information system that establishes a process for identifying configuration items throughout the system development life cycle.	The organization being inspected/assessed will develop and document a configuration management plan for the information system that establishes a process for identifying configuration items throughout the system development life cycle.	The organization conducting the inspection/assessment obtains and examines the configuration management plan to verify it establishes and documents a process for identifying configuration items throughout the system development life cycle.
CM-9	CM-9 (b)	CCI-001792	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.	The organization being inspected/assessed will implement a configuration management plan for the information system that establishes a process for identifying configuration items throughout the system development life cycle.	The organization conducting the inspection/assessment obtains and examines the configuration management plan as well as evidence of implementation (e.g., completed change requests, meeting minutes, and other relevant documents) to ensure the organization being inspected/assessed implements a configuration management plan for the information system that establishes a process for identifying configuration items throughout the system development life cycle. Checks should include verification that items being processed for CM are the items identified and that identified configuration items have not been changed without going through the documented process.
CM-9	CM-9 (b)	CCI-001793	The organization develops and documents a configuration management plan for the information system that establishes a process for managing the configuration of the configuration items.	The organization being inspected/assessed will develop and document a configuration management plan for the information system that establishes a process for managing the configuration of the configuration items.	The organization conducting the inspection/assessment obtains and examines the configuration management plan to ensure it establishes and documents a process for managing the configuration of the configuration items.
CM-9	CM-9 (b)	CCI-001795	The organization implements a configuration management plan for the information system that establishes a process for managing the configuration of the configuration items.	The organization being inspected/assessed will implement a configuration management plan that has a process for controlling changes to configuration items.	The organization conducting the inspection/assessment obtains and examines the configuration management plan as well as evidence of implementation (e.g., completed change requests, meeting minutes, and other relevant documents) to ensure the organization being inspected/assessed implements a configuration management plan for the information system that establishes a process for managing the configuration of the configuration items.

CM-9	CM-9 (c)	CCI-001796	The organization develops and documents a configuration management plan for the information system that places the configuration items under configuration management.	The organization being inspected/assessed will develop and document a configuration management plan for the information system that places the configuration items under configuration management.	The organization conducting the inspection/assessment obtains and examines the configuration management plan to ensure the organization being inspected/assessed documents that configuration items are placed under configuration management.
CM-9	CM-9 (c)	CCI-001798	The organization implements a configuration management plan for the information system that places the configuration items under configuration management.	The organization being inspected/assessed will implement a configuration management plan for the information system that places the configuration items under configuration management.	The organization conducting the inspection/assessment obtains and examines the configuration management plan as well as evidence of implementation (e.g., completed change requests, meeting minutes, and other relevant documents) to ensure the organization being inspected/assessed implements a configuration management plan for the information system and that configuration items identified are under configuration management.
CM-9	CM-9 (d)	CCI-001799	The organization develops a configuration management plan for the information system that protects the configuration management plan from unauthorized disclosure and modification.	The organization being inspected/assessed must develop and document a plan to protect the configuration management plan from unauthorized disclosure and modification. Measures must include marking, labeling, and handling to prevent improper disclosure. The organization being inspected/assessed must ensure that all changes to the CM plan are approved.	The organization conducting the inspection/assessment obtains and examines the configuration management plan to verify that it identifies the protection measures.
CM-9	CM-9 (d)	CCI-001801	The organization implements a configuration management plan for the information system that protects the configuration management plan from unauthorized disclosure and modification.	The organization being inspected/assessed must implement a plan to protect the configuration management plan from unauthorized disclosure and modification. Measures must include marking, labeling, and handling to prevent improper disclosure. The organization being inspected/assessed must ensure that all changes to the CM plan are approved.	The organization conducting the inspection/assessment obtains and examines the configuration management plan to verify that the identified protection measures are implemented.
CM-10	CM-10 (a)	CCI-001726	The organization uses software in accordance with contract agreements.	The organization being inspected/assessed uses software in accordance with contract agreements.	The organization conducting the inspection/assessment obtains and examines a sampling of contract agreements and supporting evidence concerning the usage of software to ensure compliance with the contract agreements.
CM-10	CM-10 (a)	CCI-001727	The organization uses software documentation in accordance with contract agreements.	The organization being inspected/assessed uses software documentation in accordance with contract agreements.	The organization conducting the inspection/assessment obtains and examines a sampling of contract agreements associated with software documentation and supporting evidence concerning the usage of software documentation to ensure compliance with contract agreements.
CM-10	CM-10 (a)	CCI-001728	The organization uses software in accordance with copyright laws.	The organization being inspected/assessed uses software in accordance with copyright laws.	The organization conducting the inspection/assessment obtains and examines supporting evidence concerning the usage of software to ensure compliance with copyright laws.
CM-10	CM-10 (a)	CCI-001729	The organization uses software documentation in accordance with copyright laws.	The organization being inspected/assessed uses software documentation in accordance with copyright laws.	The organization conducting the inspection/assessment obtains and examines supporting evidence concerning the usage of software documentation to ensure compliance with copyright laws.
CM-10	CM-10 (b)	CCI-001730	The organization tracks the use of software protected by quantity licenses to control copying of the software.	The organization being inspected/assessed tracks the use of software protected by quantity licenses to control copying of the software. Software license tracking can be accomplished by manual methods (e.g., simple spreadsheets) or automated methods (e.g., specialized tracking applications) depending on organizational needs.	The organization conducting the inspection/assessment obtains and examines the tracking records to ensure the organization being inspected/assessed tracks the use of software protected by quantity licenses to control copying of the software.
CM-10	CM-10 (b)	CCI-001802	The organization tracks the use of software documentation protected by quantity licenses to control copying of the software documentation.	The organization being inspected/assessed tracks the use of software documentation protected by quantity licenses to control copying of the software documentation. Software license tracking can be accomplished by manual methods (e.g., simple spreadsheets) or automated methods (e.g., specialized tracking applications) depending on organizational needs.	The organization conducting the inspection/assessment obtains and examines the tracking records to ensure the organization being inspected/assessed tracks the use of software documentation protected by quantity licenses to control copying of the software documentation.

CM-10	CM-10 (b)	CCI-001803	The organization tracks the use of software protected by quantity licenses to control distribution of the software.	The organization being inspected/assessed tracks the use of software protected by quantity licenses to control distribution of the software. Software license tracking can be accomplished by manual methods (e.g., simple spreadsheets) or automated methods (e.g., specialized tracking applications) depending on organizational needs.	The organization conducting the inspection/assessment obtains and examines the tracking records to ensure the organization being inspected/assessed tracks the use of software protected by quantity licenses to control distribution of the software.
CM-10	CM-10 (b)	CCI-001731	The organization tracks the use of software documentation protected by quantity licenses to control distribution of the software documentation.	The organization being inspected/assessed tracks the use of software documentation protected by quantity licenses to control distribution of the software documentation. Software license tracking can be accomplished by manual methods (e.g., simple spreadsheets) or automated methods (e.g., specialized tracking applications) depending on organizational needs.	The organization conducting the inspection/assessment obtains and examines the tracking records to ensure the organization being inspected/assessed tracks the use of software documentation protected by quantity licenses to control distribution of the software documentation.
CM-10	CM-10 (c)	CCI-001732	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.	The organization being inspected/assessed reviews and authorizes in order to control 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. The organization must maintain an audit trail of peer-to-peer file sharing technology reviews and authorizations.	The organization conducting the inspection/assessment obtains and examines the audit trail of peer-to-peer file sharing technology reviews and authorizations to ensure the organization being inspected/assessed 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.
CM-10	CM-10 (c)	CCI-001733	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.	The organization being inspected/assessed 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.	The organization conducting the inspection/assessment obtains and examines the documentation for 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.
CM-10 (1)	CM-10 (1)	CCI-001734	The organization defines the restrictions to be followed on the use of open source software.	DoD has defined the restrictions as IAW DoD Memorandum "Clarifying Guidance Regarding Open Source Software (OSS)" 16 Oct 2009 (http://dodcio.defense.gov/Home/Issuances/DoDCIOMemorandums.aspx).	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the restrictions as IAW DoD Memorandum "Clarifying Guidance Regarding Open Source Software (OSS)" 16 Oct 2009 (http://dodcio.defense.gov/Home/Issuances/DoDCIOMemorandums.aspx).
CM-10 (1)	CM-10 (1)	CCI-001735	The organization establishes organization-defined restrictions on the use of open source software.	DoD Memorandum "Clarifying Guidance Regarding Open Source Software (OSS)" 16 Oct 2009 (http://dodcio.defense.gov/Home/Issuances/DoDCIOMemorandums.aspx) meets the DoD requirement for establishing restrictions on the use of open source software. DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoD Memorandum "Clarifying Guidance Regarding Open Source Software (OSS)."	DoD Memorandum "Clarifying Guidance Regarding Open Source Software (OSS)" 16 Oct 2009 (http://dodcio.defense.gov/Home/Issuances/DoDCIOMemorandums.aspx) meets the DoD requirement for establishing restrictions on the use of open source software. DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoD Memorandum "Clarifying Guidance Regarding Open Source Software (OSS)."
CM-11	CM-11 (a)	CCI-001804	The organization defines the policies for governing the installation of software by users.	The organization being inspected/assessed must define policies governing the installation of software by users. DoD has determined the policies are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines policies governing the installation of software by users (e.g., user agreements, CM plan, etc.) to ensure the organization being inspected/assessed defines the policies for governing the installation of software by users. DoD has determined the policies are not appropriate to define at the Enterprise level.
CM-11	CM-11 (a)	CCI-001805	The organization establishes organization-defined policies governing the installation of software by users.	The organization being inspected/assessed documents their policies governing the installation of software by users (e.g., user agreements, CM plan, etc.).	The organization conducting the inspection/assessment obtains and examines documented policies governing the installation of software by users (e.g., user agreements, CM plan, etc.) to ensure the organization being inspected/assessed establishes policies governing the installation of software by users.
CM-11	CM-11 (b)	CCI-001806	The organization defines methods to be employed to enforce the software installation policies.	The organization being inspected/assessed must define and document the methods employed to enforce the software installation policies. DoD has determined the policies are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines documentation of the methods employed to ensure the organization being inspected/assessed defines methods to be employed to enforce the software installation policies. DoD has determined the policies are not appropriate to define at the Enterprise level.

CM-11	CM-11 (b)	CCI-001807	The organization enforces software installation policies through organization-defined methods.	The organization being inspected/assessed must enforce software installation policies as defined in CM-11, CCI 1804 through methods defined in CM-11, CCI 1806.	The organization conducting the inspection/assessment obtains and examines software installation policies defined in CM-11, CCI 1804 and inspects the methods defined in CM-11, CCI 1806 to verify they are properly implemented.
CM-11	CM-11 (c)	CCI-001808	The organization defines the frequency on which it will monitor software installation policy compliance.	DoD has defined the frequency as at least monthly.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as at least monthly.
CM-11	CM-11 (c)	CCI-001809	The organization monitors software installation policy compliance per organization-defined frequency.	The organization being inspected/assessed must monitor software installation policy compliance at least monthly. The organization must maintain audit trails of monitoring activity. DoD has defined the frequency as at least monthly.	The organization conducting the inspection/assessment obtains and examines the audit trails of monitoring activities to ensure the organization being inspected/assessed monitors software installation policy compliance at least monthly. DoD has defined the frequency as at least monthly.
CM-11 (2)	CM-11 (2)	CCI-001812	The information system prohibits user installation of software without explicit privileged status.	The organization being inspected/assessed must configure the information system to prevent the installation of software by non-privileged users. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1812.	The organization conducting the inspection/assessment obtains and examines the configuration of the information system components to ensure that installation of software without explicit privileged status is prohibited. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1812.
CP-1	CP-1 (a) (1)	CCI-002825	The organization defines personnel or roles to whom the contingency planning policy is to be disseminated.	DoD has defined the personnel or roles as all stakeholders identified in the contingency plan.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as all stakeholders identified in the contingency plan.
CP-1	CP-1 (a) (1)	CCI-000438	The organization develops and documents a contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	DoDI 8500.01 and NIST SP 800-34 meet the DoD requirements for contingency planning policy and procedures. DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8500.01 and NIST SP 800-34.	DoDI 8500.01 and NIST SP 800-34 meet the DoD requirements for contingency planning policy and procedures. DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8500.01 and NIST SP 800-34.
CP-1	CP-1 (a) (1)	CCI-000439	The organization disseminates a contingency planning policy to organization-defined personnel or roles.	DoD disseminates DoDI 8500.01 organization-wide via the DoD Issuances website. http://www.dtic.mil/whs/directives/corres/dir.html NIST disseminates NIST SP 800-34 via http://csrc.nist.gov/publications/PubsSPs.html	DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8500.01 and NIST SP 800-34.
CP-1	CP-1 (a) (2)	CCI-002826	The organization defines personnel or roles to whom the contingency planning procedures are disseminated.	DoD has defined the personnel or roles as all stakeholders identified in the contingency plan.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as all stakeholders identified in the contingency plan.
CP-1	CP-1 (a) (2)	CCI-000441	The organization develops and documents procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.	DoDI 8500.01 and NIST SP 800-34 meet the DoD requirements for contingency planning policy and procedures. DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8500.01 and NIST SP 800-34.	DoDI 8500.01 and NIST SP 800-34 meet the DoD requirements for contingency planning policy and procedures. DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8500.01 and NIST SP 800-34.
CP-1	CP-1 (a) (2)	CCI-001597	The organization disseminates contingency planning procedures to organization-defined personnel or roles.	DoD disseminates DoDI 8500.01 organization-wide via the DoD Issuances website. http://www.dtic.mil/whs/directives/corres/dir.html NIST disseminates NIST SP 800-34 via http://csrc.nist.gov/publications/PubsSPs.html	DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8500.01 and NIST SP 800-34.
CP-1	CP-1 (b) (1)	CCI-000437	The organization defines the frequency to review and update the current contingency planning policy.	DoD has defined the frequency as every 5 years.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every 5 years.

CP-1	CP-1 (b) (1)	CCI-000440	The organization reviews and updates the current contingency planning policy in accordance with organization-defined frequency.	DoDI 8500.01 and NIST SP 800-34 meet the DoD requirements for contingency planning policy and procedures. DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8500.01 and NIST SP 800-34.	DoDI 8500.01 and NIST SP 800-34 meet the DoD requirements for contingency planning policy and procedures. DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8500.01 and NIST SP 800-34.
CP-1	CP-1 (b) (2)	CCI-001596	The organization defines the frequency to review and update the current contingency planning procedures.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.
CP-1	CP-1 (b) (2)	CCI-001598	The organization reviews and updates the current contingency planning procedures in accordance with the organization-defined frequency.	DoDI 8500.01 and NIST SP 800-34 meet the DoD requirements for contingency planning policy and procedures. DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8500.01 and NIST SP 800-34.	DoDI 8500.01 and NIST SP 800-34 meet the DoD requirements for contingency planning policy and procedures. DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8500.01 and NIST SP 800-34.
CP-2	CP-2 (a) (1)	CCI-000443	The organization develops a contingency plan for the information system that identifies essential missions.	The organization being inspected/assessed must clearly and accurately document essential missions for its information system(s). Impact of loss of essential mission functions must be defined using CNSSI 1253.	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents essential missions for its information system(s).
CP-2	CP-2 (a) (1)	CCI-000444	The organization develops a contingency plan for the information system that identifies essential business functions.	The organization being inspected/assessed must clearly and accurately document essential business functions for its information system(s). Impact of loss of essential business functions must be defined using CNSSI 1253.	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents essential business functions for its information system(s).
CP-2	CP-2 (a) (1)	CCI-000445	The organization develops a contingency plan for the information system that identifies associated contingency requirements.	The organization being inspected/assessed must clearly and accurately document associated contingency requirements for its information system(s).	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents associated contingency requirements for its information system(s).
CP-2	CP-2 (a) (2)	CCI-000446	The organization develops a contingency plan for the information system that provides recovery objectives.	The organization being inspected/assessed must clearly and accurately document recovery objectives for its information system(s).	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents recovery objectives for its information system(s).
CP-2	CP-2 (a) (2)	CCI-000447	The organization develops a contingency plan for the information system that provides restoration priorities.	The organization being inspected/assessed must clearly and accurately document restoration priorities for its information system(s).	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents restoration priorities for its information system(s).
CP-2	CP-2 (a) (2)	CCI-000448	The organization develops a contingency plan for the information system that provides metrics.	The organization being inspected/assessed must clearly and accurately document metrics for its information system(s).	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents metrics for its information system(s).
CP-2	CP-2 (a) (3)	CCI-000449	The organization develops a contingency plan for the information system that addresses contingency roles, responsibilities, assigned individuals with contact information.	The organization being inspected/assessed must clearly and accurately document contingency roles, responsibilities, assigned individuals with contact information for its information system(s).	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents contingency roles, responsibilities, assigned individuals with contact information for its information system(s).
CP-2	CP-2 (a) (4)	CCI-000450	The organization develops a contingency plan for the information system that addresses maintaining essential missions despite an information system disruption.	The organization being inspected/assessed must clearly and accurately document maintaining essential missions despite an information system disruption for its information system(s).	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents maintaining essential missions despite an information system disruption for its information system(s).
CP-2	CP-2 (a) (4)	CCI-000451	The organization develops a contingency plan for the information system that addresses maintaining essential business functions despite an information system disruption.	The organization being inspected/assessed must clearly and accurately document maintaining business functions despite an information system disruption for its information system(s).	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents maintaining business functions despite an information system disruption for its information system(s).
CP-2	CP-2 (a) (4)	CCI-000452	The organization develops a contingency plan for the information system that addresses maintaining essential missions despite an information system compromise.	The organization being inspected/assessed must clearly and accurately document maintaining essential missions despite an information system compromise for its information system(s).	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents maintaining essential missions despite an information system compromise for its information system(s).
CP-2	CP-2 (a) (4)	CCI-000453	The organization develops a contingency plan for the information system that addresses maintaining essential business functions despite an information system compromise.	The organization being inspected/assessed must clearly and accurately document maintaining business functions despite an information system compromise for its information system(s).	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents maintaining business functions despite an information system compromise for its information system(s).
CP-2	CP-2 (a) (4)	CCI-000454	The organization develops a contingency plan for the information system that addresses maintaining essential missions despite an information system failure.	The organization being inspected/assessed must clearly and accurately document maintaining essential missions despite an information system failure for its information system(s).	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents maintaining essential missions despite an information system failure for its information system(s).

CP-2	CP-2 (a) (4)	CCI-000455	The organization develops a contingency plan for the information system that addresses maintaining essential business functions despite an information system failure.	The organization being inspected/assessed must clearly and accurately document maintaining business functions despite an information system failure for its information system(s).	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents maintaining business functions despite an information system failure for its information system(s).
CP-2	CP-2 (a) (5)	CCI-000456	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.	The organization being inspected/assessed must clearly and accurately document eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented for its information system(s).	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented for its information system(s).
CP-2	CP-2 (a) (6)	CCI-000457	The organization develops a contingency plan for the information system that is reviewed and approved by organization-defined personnel or roles.	The organization being inspected/assessed reviews and approves the contingency plan by at a minimum, the ISSM and ISSO. The organization must maintain an audit trail of the review and approval activity. DoD has defined the personnel or roles as at a minimum, the ISSM and ISSO.	The organization conducting the inspection/assessment obtains and examines the audit trail to ensure the contingency plan has been reviewed and approved by at a minimum, the ISSM and ISSO. DoD has defined the personnel or roles as at a minimum, the ISSM and ISSO.
CP-2	CP-2 (b)	CCI-000458	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.	DoD has defined the list as all stakeholders identified in the contingency plan.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the list as all stakeholders identified in the contingency plan.
CP-2	CP-2 (b)	CCI-000459	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.	The organization being inspected/assessed ensures the contingency plan is disseminated to all stakeholders identified in the contingency plan via an information sharing capibility. DoD has defined the list as all stakeholders identified in the contingency plan.	The organization conducting the inspection/assessment obtains and examines the contingency plan via the inspected organization's information sharing capability (e.g. portal, intranet, email, etc.) to ensure it has been disseminated.
CP-2	CP-2 (c)	CCI-000460	The organization coordinates contingency planning activities with incident handling activities.	The organization being inspected/assessed will coordinate the contingency plan and incident response plan (IR-8) to ensure they do not contradict each other's objectives or result in duplicate efforts/activities.	The organization conducting the inspection/assessment obtains and examines the contingency plan and the incident response plan (IR-8) to ensure they do not contradict each other's objectives or result in duplicate efforts/activities.
CP-2	CP-2 (d)	CCI-000461	The organization defines the frequency to review the contingency plan for the information system.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.
CP-2	CP-2 (d)	CCI-000462	The organization reviews the contingency plan for the information system in accordance with organization-defined frequency.	The organization being inspected/assessed annually reviews the contingency plan. The organization must maintain an audit trail of annual reviews.	The organization conducting the inspection/assessment obtains and examines the audit trail to ensure the contingency plan is reviewed annually.
CP-2	CP-2 (e)	CCI-000463	The organization updates the contingency plan to address changes to the organization.	The organization being inspected/assessed must clearly and accurately update the contingency plan to address organizational changes. The organization must document the update activities as an audit trail.	The organization conducting the inspection/assessment obtains and examines the contingency plan and audit trail to ensure the organization clearly and accurately updates the contingency plan to address organizational changes.
CP-2	CP-2 (e)	CCI-000464	The organization updates the contingency plan to address changes to the information system.	The organization being inspected/assessed must clearly and accurately update the contingency plan to address changes to the information system. The organization must document the update activities as an audit trail.	The organization conducting the inspection/assessment obtains and examines the contingency plan and audit trail to ensure the organization clearly and accurately updates the contingency plan to address information system changes.
CP-2	CP-2 (e)	CCI-000465	The organization updates the contingency plan to address changes to the environment of operation.	The organization being inspected/assessed must clearly and accurately revise the contingency plan to address changes to the environment of operation. The organization must document the update activities as an audit trail.	The organization conducting the inspection/assessment obtains and examines the contingency plan and audit trail to ensure the organization clearly and accurately revises the contingency plan to address changes to the environment of operation.
CP-2	CP-2 (e)	CCI-000466	The organization updates the contingency plan to address problems encountered during contingency plan implementation, execution, or testing.	The organization being inspected/assessed must clearly and accurately revise the contingency plan to address problems encountered during contingency plan implementation, execution, or testing. The organization must document the update activities as an audit trail.	The organization conducting the inspection/assessment obtains and examines the contingency plan and audit trail to ensure the organization clearly and accurately revises the contingency plan to address problems encountered during contingency plan implementation, execution, or testing.

CP-2	CP-2 (f)	CCI-000468	The organization communicates contingency plan changes to organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements.	The organization being inspected/assessed communicates contingency plan changes to all stakeholders identified in the contingency plan. DoD has defined the list as all stakeholders identified in the contingency plan.	The organization conducting the inspection/assessment examines the contingency plan via the inspected organization's information sharing capability (e.g. portal, intranet, email, etc.) to ensure the most current version has been communicated.
CP-2	CP-2 (a) (6)	CCI-002830	The organization defines the personnel or roles who review and approve the contingency plan for the information system.	DoD has defined the personnel or roles as at a minimum, the ISSM and ISSO.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as at a minimum, the ISSM and ISSO.
CP-2	CP-2 (f)	CCI-002831	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.	DoD has defined the list as all stakeholders identified in the contingency plan	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the list as all stakeholders identified in the contingency plan
CP-2	CP-2 (g)	CCI-002832	The organization protects the contingency plan from unauthorized disclosure and modification.	The organization being inspected/assessed documents and implements a process to protect the contingency plan from unauthorized disclosure and modification.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed protects the contingency plan from unauthorized disclosure and modification.
CP-3	CP-3 (a)	CCI-002833	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.	DoD has defined the time period as at a maximum, 10 working days.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as at a maximum, 10 working days.
CP-3	CP-3 (a)	CCI-000486	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.	The organization being inspected/assessed provides initial contingency training to personnel with contigency roles and responsibilities IAW CP-2, CCI 449 at a maximum, 10 working days of assuming a contingency role or responsibility. The organization will maintain documentation of the training activity dates, location, and personnel for audit trail purposes and future reference (e.g., scheduling refresher training, etc.). DoD has defined the time period as at a maximum, 10 working days.	The organization conducting the inspection/assessment obtains and examines the list of contingency personnel and documentation of initial contingency training for the purpose of ensuring that all personnel with contingency roles and responsibilities have received initial contingency training at a maximum, 10 working days of assuming a contingency role or responsibility. DoD has defined the time period as at a maximum, 10 working days.
CP-3	CP-3 (b)	CCI-002834	The organization provides contingency training to information system users consistent with assigned roles and responsibilities when required by information system changes.	The organization being inspected/assessed will update contingency training materials when required by information system changes and provide that training to personnel with contingency roles and responsibilities IAW CP-2, CCI 449. The organization will maintain documentation of the training activity dates, location, and personnel for audit trail purposes and future reference (e.g., scheduling refresher training, etc.).	The organization conducting the inspection/assessment obtains and examines training materials and documentation of training activities to determine whether the materials are accurate in consideration of the state of the information system and content of the contingency plan. The organization ensures that training is provided to users consistent with assigned roles and responsibilities.
CP-3	CP-3 (c)	CCI-000485	The organization defines the frequency of refresher contingency training to information system users.	DoD has defined the frequency as at least annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as at least annually
CP-3	CP-3 (c)	CCI-000487	The organization provides refresher contingency training to information system users consistent with assigned roles and responsibilities in accordance with organization-defined frequency.	The organization being inspected/assessed provides refresher contingency training to personnel with contingency roles and responsibilities IAW CP-2, CCI 449 at least annually. The organization will maintain documentation of the training activity dates, location, and personnel for audit trail purposes and future reference (e.g., scheduling refresher training, etc.). DoD has defined the frequency as at least annually.	The organization conducting the inspection/assessment obtains and examines the list of contingency personnel and documentation of refresher contingency training for the purpose of ensuring that all personnel with contingency roles and responsibilities have received refresher contingency training at least annually. DoD has defined the frequency as at least annually.
CP-4	CP-4 (a)	CCI-000490	The organization defines the frequency to test the contingency plan for the information system.	DoD has defined the frequency as at least annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as at least annually.

CP-4	CP-4 (a)	CCI-000492	The organization defines contingency plan tests to be conducted for the information system.	The organization being inspected/assessed defines and documents contingency plan tests to be conducted for the information system. DoD has determined the contingency plan tests are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented contingency plan tests to ensure the organization being inspected/assessed defines contingency plan tests to be conducted for the information system. DoD has determined the contingency plan tests are not appropriate to define at the Enterprise level.
CP-4	CP-4 (a)	CCI-000494	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.	The organization being inspected/assessed conduct tests defined in CP-4, 492 at least annually to determine the effectiveness of the plan and the organizational readiness to execute the plan. The organization must maintain a record of test results. DoD has defined the frequency as at least annually.	The organization conducting the inspection/assessment obtains and examines the record of test results to ensure the organization being inspected/assessed conduct tests defined in CP-4, 492 at least annually to determine the effectiveness of the plan and the organizational readiness to execute the plan. DoD has defined the frequency as at least annually.
CP-4	CP-4 (b)	CCI-000496	The organization reviews the contingency plan test results.	The organization being inspected/assessed will review the contingency plan test results. The organization must maintain an audit trail of issues identified during the reviews of the contingency plan test results.	The organization conducting the inspection/assessment obtains and examines the audit trail of issues identified during the reviews of the contingency plan test results to ensure the organization being inspected/assessed reviews the contingency plan test results.
CP-4	CP-4 (c)	CCI-000497	The organization initiates corrective actions, if needed, after reviewing the contingency plan test results.	The organization being inspected/assessed identifies and documents any corrective actions required after reviewing the contingency plan test results. The organization initiates corrective actions and tracks those actions within the POA&M.	The organization conducting the inspection/assessment obtains and examines the contingency plan test results as well as any documented corrective actions required and ensures the corrective actions are being implemented and tracked within the POA&M.
CP-9	CP-9 (a)	CCI-000534	The organization defines frequency of conducting user-level information backups to support recovery time objectives and recovery point objectives.	DoD has defined the frequency as at least weekly as defined in the contingency plan.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as at least weekly as defined in the contingency plan.
CP-9	CP-9 (a)	CCI-000535	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.	The organization being inspected/assessed must identify user level information within the backup strategy and configure the system to perform backups at least weekly as defined in the contingency plan.	The organization conducting the inspection/assessment obtains and reviews the backup strategy, and examines a sample of systems to ensure they are configured to perform back ups at least weekly as defined in the contingency plan.
CP-9	CP-9 (b)	CCI-000536	The organization defines frequency of conducting system-level information backups to support recovery time objectives and recovery point objectives.	DoD has defined the frequency as at least weekly and as required by system baseline configuration changes in accordance with the contingency plan.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as at least weekly and as required by system baseline configuration changes in accordance with the contingency plan.
CP-9	CP-9 (b)	CCI-000537	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.	The organization being inspected/assessed must identify system-level information within the backup strategy and configure the system to perform backups at least weekly and as required by system baseline configuration changes in accordance with the contingency plan.	The organization conducting the inspection/assessment obtains and reviews the backup strategy, and examines a sample of systems to ensure they are configured to perform back ups at least weekly and as required by system baseline configuration changes in accordance with the contingency plan.
CP-9	CP-9 (c)	CCI-000538	The organization defines the frequency of conducting information system documentation backups including security-related documentation to support recovery time objectives and recovery point objectives.	DoD has defined the frequency as when created or received, when updated, and as required by system baseline configuration changes in accordance with the contingency plan.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as when created or received, when updated, and as required by system baseline configuration changes in accordance with the contingency plan.
CP-9	CP-9 (c)	CCI-000539	The organization conducts backups of information system documentation including security-related documentation per organization-defined frequency that is consistent with recovery time and recovery point objectives.	The organization being inspected/assessed conducts backups of information system documentation including security-related documentation when created or received, when updated, and as required by system baseline configuration changes in accordance with the contingency plan.	The organization conducting the inspection/assessment obtains and examines the latest version of the information system documentation including security-related documentation to verify it is the same version as contained in backups.
CP-9	CP-9 (d)	CCI-000540	The organization protects the confidentiality, integrity, and availability of backup information at storage locations.	The organization being inspected/assessed will protect the confidentiality, integrity, and availability of backup information at the storage location IAW the system security plan.	The organization conducting the inspection/assessment obtains and examines the system security plan and ensures backup information at the storage location is protected IAW the system security plan.

CP-10	CP-10	CCI-000550	The organization provides for the recovery and reconstitution of the information system to a known state after a disruption.	The organization being inspected/assessed provides automated mechanisms or manual procedures, or a combination of the two, for the recovery and reconstitution of its information system to a known state after a disruption. The organization must identify the selected method in the contingency plan.	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it identifies the recovery and reconstitution method for its information system to a known state after a disruption.
CP-10	CP-10	CCI-000551	The organization provides for the recovery and reconstitution of the information system to a known state after a compromise.	The organization being inspected/assessed provides automated mechanisms or manual procedures, or a combination of the two, for the recovery and reconstitution of its information system to a known state after a compromise. The organization must identify the selected method in the contingency plan.	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it identifies the recovery and reconstitution method for its information system to a known state after a compromise.
CP-10	CP-10	CCI-000552	The organization provides for the recovery and reconstitution of the information system to a known state after a failure.	The organization being inspected/assessed provides automated mechanisms or manual procedures, or a combination of the two, for the recovery and reconstitution of its information system to a known state after a failure. The organization must identify the selected method in the contingency plan.	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it identifies the recovery and reconstitution method for its information system to a known state after a failure.
IA-1	IA-1 (a)	CCI-001933	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.	DoD has defined the roles to be recipients of the identification and authentication policy and the procedures as the ISSO and ISSM and others as the local organization deems appropriate. DoDI 8520.02 and DoDI 8520.03 meet the DoD requirement for Identification and Authentication policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 8520.02 and DoDI 8520.03.	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8520.02 and DoDI 8520.03. DoD has defined the roles to be recipients of the identification and authentication policy and the procedures as the ISSO and ISSM and others as the local organization deems appropriate.
IA-1	IA-1 (a) (1)	CCI-000756	The organization develops and documents an identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	DoD developed DoDI 8520.02 and DoDI 8520.03 as the identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 8520.02 and DoDI 8520.03.	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8520.02 and DoDI 8520.03.
IA-1	IA-1 (a) (1)	CCI-000757	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.	DoD disseminates the DoDI 8520.02 and DoDI 8520.03 via the DoD Issuances website (http://www.dtic.mil/whs/directives/corres/dir.html) to the ISSO and ISSM and others as the local organization deems appropriate as an identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 8520.02 and DoDI 8520.03. DoD has defined the personnel or roles to be recipients of the identification and authentication policy and the procedures as the ISSO and ISSM and others as the local organization deems appropriate.	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8520.02 and DoDI 8520.03. DoD has defined the personnel or roles to be recipients of the identification and authentication policy and the procedures as the ISSO and ISSM and others as the local organization deems appropriate.

IA-1	IA-1 (a) (2)	CCI-000760	The organization develops and documents procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.	DoD develops within DoDI 8520.02 and DoDI 8520.03, procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8520.02 and DoDI 8520.03.	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8520.02 and DoDI 8520.03.
IA-1	IA-1 (a) (2)	CCI-000761	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.	DoD disseminates the DoDI 8520.02 and DoDI 8520.03 to the ISSO and ISSM and others as the local organization deems appropriate via the DoD Issuances website (http://www.dtic.mil/whs/directives/corres/dir.html). DoDI 8520.02 and DoDI 8520.03 are procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 8520.02 and DoDI 8520.03. DoD has defined the personnel or roles to be recipients of the identification and authentication policy and the procedures as the ISSO and ISSM and others as the local organization deems appropriate.	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8520.02 and DoDI 8520.03. DoD has defined the personnel or roles to be recipients of the identification and authentication policy and the procedures as the ISSO and ISSM and others as the local organization deems appropriate.
IA-1	IA-1 (b) (1)	CCI-000758	The organization reviews and updates identification and authentication policy in accordance with the organization defined frequency.	DoD reviews and updates identification and authentication policy (DoDI 8520.02 and DoDI 8520.03) annually. DoD Components are automatically compliant with this CCI because they are covered at the DoD level policies, DoDI 8520.02 and DoDI 8520.03. DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8520.02 and DoDI 8520.03. DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.
IA-1	IA-1 (b) (1)	CCI-000759	The organization defines a frequency for reviewing and updating the identification and authentication policy.	DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.
IA-1	IA-1 (b) (2)	CCI-000762	The organization reviews and updates identification and authentication procedures in accordance with the organization defined frequency.	DoD reviews and updates identification and authentication procedures (DoDI 8520.02 and DoDI 8520.03) annually. The organization being inspected/assessed is automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 8520.02 and DoDI 8520.03. DoD has defined the frequency as reviewed annually - updated as appropriate.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 8520.02 and DoDI 8520.03. DoD has defined the frequency as reviewed annually - updated as appropriate.
IA-1	IA-1 (b) (2)	CCI-000763	The organization defines a frequency for reviewing and updating the identification and authentication procedures.	DoD has defined the frequency as reviewed annually - updated as appropriate.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as reviewed annually - updated as appropriate.
IA-2	IA-2	CCI-000764	The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).	The organization being inspected/assessed configures the information system to uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 764.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users). For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 764.

IA-2 (1)	IA-2 (1)	CCI-000765	The information system implements multifactor authentication for network access to privileged accounts.	The organization being inspected/assessed configures the information system to implement multifactor authentication for network access to privileged accounts. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 765.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement multifactor authentication for network access to privileged accounts. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 765.
IA-2 (2)	IA-2 (2)	CCI-000766	The information system implements multifactor authentication for network access to non-privileged accounts.	The organization being inspected/assessed configures the information system to implement multifactor authentication for network access to non-privileged accounts. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 766.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement multifactor authentication for network access to non-privileged accounts. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 766.
IA-2 (5)	IA-2 (5)	CCI-000770	The organization requires individuals to be authenticated with an individual authenticator when a group authenticator is employed.	The organization being inspected/assessed requires individuals or configures the information system to require individuals to be authenticated with an individual authenticator when a group authenticator is employed. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 770.	The organization conducting the inspection/assessment obtains and examines standard operating procedures or system documentation to ensure the organization being inspected/assessed requires individuals to be authenticated with an individual authenticator when a group authenticator is employed. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 770.
IA-2 (8)	IA-2 (8)	CCI-001941	The information system implements replay-resistant authentication mechanisms for network access to privileged accounts.	The organization being inspected/assessed configures the information system to implement replay-resistant authentication mechanisms for network access to privileged accounts. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1941.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement replay-resistant authentication mechanisms for network access to privileged accounts. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1941.
IA-2 (11)	IA-2 (11)	CCI-001947	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.	For the strength of mechanism requirements DoD has defined requirements as DoD PKI or a technology approved by their Authorizing Official, FIPS 140-2, NIAP Certification, or NSA approval.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. For the strength of mechanism requirements DoD has defined requirements as DoD PKI or a technology approved by their Authorizing Official, FIPS 140-2, NIAP Certification, or NSA approval.
IA-2 (11)	IA-2 (11)	CCI-001950	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.	For the strength of mechanism requirements DoD has defined requirements as DoD PKI or a technology approved by their Authorizing Official, FIPS 140-2, NIAP Certification, or NSA approval.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. For the strength of mechanism requirements DoD has defined requirements as DoD PKI or a technology approved by their Authorizing Official, FIPS 140-2, NIAP Certification, or NSA approval.

IA-2 (11)	IA-2 (11)	CCI-001948	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.	The organization being inspected/assessed configures the information system to implement 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. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1948.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement 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. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1948.
IA-2 (11)	IA-2 (11)	CCI-001952	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.	The organization being inspected/assessed will use DoD PKI or a technology approved by their Authorizing Official that meet Federal standards for authentication such as FIPS 140-2, NIAP Certification, or NSA approval. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1952.	The organization conducting the inspection/assessment obtains and examines the device used to ensure that the device implemented for multifactor authentication for remote access to non-privileged accounts meets Federal standards for authentication such as FIPS 140-2, NIAP Certification, or NSA approval. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1952.
IA-2 (11)	IA-2 (11)	CCI-001951	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.	The organization being inspected/assessed configures the information system to implement 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. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1951.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement 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. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1951.
IA-2 (11)	IA-2 (11)	CCI-001949	The device used in the information system implementation of multifactor authentication for remote access to privileged accounts meets organization-defined strength of mechanism requirements.	The organization being inspected/assessed will use DoD PKI or a technology approved by their Authorizing Official that meet Federal standards for authentication such as FIPS 140-2, NIAP Certification, or NSA approval. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1949.	The organization conducting the inspection/assessment obtains and examines the device used to ensure that the device implemented for multifactor authentication for remote access to privileged accounts meets Federal standards for authentication such as FIPS 140-2, NIAP Certification, or NSA approval. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1949.
IA-2 (12)	IA-2 (12)	CCI-001953	The information system accepts Personal Identity Verification (PIV) credentials.	The organization being inspected/assessed configures the information system to accept PIV/CAC authentication. This control enhancement applies to organizations implementing logical access control systems (LACS) and physical access control systems (PACS). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1953	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to accept PIV/CAC authentication. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1953.

IA-2 (12)	IA-2 (12)	CCI-001954	The information system electronically verifies Personal Identity Verification (PIV) credentials.	The organization being inspected/assessed configures the information system to verify PIV/CAC authentication. This control enhancement applies to organizations implementing logical access control systems (LACS) and physical access control systems (PACS). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1954.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to verify PIV/CAC authentication. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1954.
IA-3	IA-3	CCI-000777	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.	DoD has defined the value as all mobile devices and network connected endpoint devices (including but not limited to: workstations, printers, servers (outside a datacenter), VoIP Phones, VTC CODECs).	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the value as all mobile devices and network connected endpoint devices (including but not limited to: workstations, printers, servers (outside a datacenter), VoIP Phones, VTC CODECs).
IA-3	IA-3	CCI-000778	The information system uniquely identifies an organization defined list of specific and/or types of devices before establishing a local, remote, or network connection.	The organization being inspected/assessed configures the network infrastructure to identify all mobile devices and network connected endpoint devices (including but not limited to: workstations, printers, servers (outside a datacenter), VoIP Phones, VTC CODECs) before establishing a local, remote, network connection. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 778. DoD has defined the value as all mobile devices and network connected endpoint devices (including but not limited to: workstations, printers, servers (outside a datacenter), VoIP Phones, VTC CODECs).	The organization conducting the inspection/assessment examine a sampling of the network infrastructure device configurations to ensure devices connecting to the infrastructure are uniquely identified. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 778.
IA-3	IA-3	CCI-001958	The information system authenticates an organization defined list of specific and/or types of devices before establishing a local, remote, or network connection.	The organization being inspected/assessed configures the network infrastructure to authenticate all mobiles devices and network connected endpoint devices (including but not limited to: workstations, printers, servers (outside a datacenter), VoIP Phones, VTC CODECs) before establishing a local, remote, network connection. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1958. DoD has defined the value as all mobile devices and network connected endpoint devices (including but not limited to: workstations, printers, servers (outside a datacenter), VoIP Phones, VTC CODECs).	The organization conducting the inspection/assessment examine a sampling of the network infrastructure device configurations to ensure devices connecting to the infrastructure are uniquely authenticated. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1958.
IA-4	IA-4 (a)	CCI-001970	The organization defines the personnel or roles that authorize the assignment of individual, group, role, and device identifiers.	DoD has defined the personnel or roles as the ISSM or ISSO.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as the ISSM or ISSO.
IA-4	IA-4 (a)	CCI-001971	The organization manages information system identifiers by receiving authorization from organization-defined personnel or roles to assign an individual, group, role or device identifier.	The organization being inspected/assessed implements a process to manage information system identifiers by receiving authorization from the ISSM or ISSO to assign an individual, group, role or device identifier. DoD has defined the personnel or roles as the ISSM or ISSO.	The organization conducting the inspection/assessment obtains and examines documentation and system configuration information to ensure the organization being inspected/assessed manages information system identifiers by receiving authorization from the ISSM or ISSO to assign an individual, group, role or device identifier. DoD has defined the personnel or roles as the ISSM or ISSO.

IA-4	IA-4 (b)	CCI-001972	The organization manages information system identifiers by selecting an identifier that identifies an individual, group, role, or device.	The organization being inspected/assessed implements a process to manage information system identifiers by selecting an identifier that identifies an individual, group, role, or device.	The organization conducting the inspection/assessment obtains and examines documentation or system configuration information to ensure the organization being inspected/assessed manages information system identifiers by selecting an identifier that identifies an individual, group, role, or device.
IA-4	IA-4 (c)	CCI-001973	The organization manages information system identifiers by assigning the identifier to the intended individual, group, role, or device.	The organization being inspected/assessed implements a process to manage information system identifiers by assigning the identifier to the intended individual, group, role, or device.	The organization conducting the inspection/assessment obtains and examines documentation or system configuration information to ensure the organization being inspected/assessed manages information system identifiers by assigning the identifier to the intended individual, group, role, or device.
IA-4	IA-4 (d)	CCI-001974	The organization defines the time period for which the reuse of identifiers is prohibited.	DoD has defined the time period as 1 year for user identifiers (DoD is not going to specify value for device identifier).	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as 1 year for user identifiers (DoD is not going to specify value for device identifier).
IA-4	IA-4 (d)	CCI-001975	The organization manages information system identifiers by preventing reuse of identifiers for an organization-defined time period.	The organization being inspected/assessed implements a process for information system identifiers to prevent reuse of identifiers for 1 year for user identifiers (DoD is not going to specify value for device identifier). DoD has defined the time period as 1 year for user identifiers (DoD is not going to specify value for device identifier).	The organization conducting the inspection/assessment obtains and examines documentation or system configuration information to ensure the organization being inspected/assessed prevents the reuse of identifiers for 1 year for user identifiers (DoD is not going to specify value for device identifier). DoD has defined the time period as 1 year for user identifiers (DoD is not going to specify value for device identifier).
IA-4	IA-4 (e)	CCI-000794	The organization defines a time period of inactivity after which the identifier is disabled.	DoD has defined the time period as 35 days of inactivity.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as 35 days of inactivity.
IA-4	IA-4 (e)	CCI-000795	The organization manages information system identifiers by disabling the identifier after an organization defined time period of inactivity.	The organization being inspected/assessed configures the information system to disable identifiers after 35 days of inactivity. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 795. DoD has defined the time period as 35 days of inactivity.	The organization conducting the inspection/assessment examines the information system configuration to ensure that identifiers are disabled after 35 days of inactivity. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 795. DoD has defined the time period as 35 days of inactivity.
IA-4 (4)	IA-4 (4)	CCI-000800	The organization defines characteristics for identifying individual status.	DoD has defined the characteristics as contractor or government employee and by nationality. User identifiers will follow the same format as DoD user e-mail addresses (john.smith.ctr@army.mil or john.smith.uk@army.mil); - DoD user e-mail display names (e.g., John Smith, Contractor <john.smith.ctr@army.mil> or John Smith, United Kingdom <john.smith.uk@army.mil>); and - automated signature blocks (e.g., John Smith, Contractor, J-6K, Joint Staff or John Doe, Australia, LNO, Combatant Command). Contractors who are also foreign nationals are identified as both, e.g., john.smith.ctr.uk@army.mil	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the characteristics as contractor or government employee and by nationality. User identifiers will follow the same format as DoD user e-mail addresses (john.smith.ctr@army.mil or john.smith.uk@army.mil); - DoD user e-mail display names (e.g., John Smith, Contractor <john.smith.ctr@army.mil> or John Smith, United Kingdom <john.smith.uk@army.mil>); and - automated signature blocks (e.g., John Smith, Contractor, J-6K, Joint Staff or John Doe, Australia, LNO, Combatant Command). Contractors who are also foreign nationals are identified as both, e.g., john.smith.ctr.uk@army.mil

IA-4 (4)	IA-4 (4)	CCI-000801	The organization manages individual identifiers by uniquely identifying each individual as organization-defined characteristic identifying individual status.	The organization being inspected/assessed documents and implements a process to manage individual identifiers by uniquely identifying each individual as contractor or government employee and by nationality. User identifiers will follow the same format as DoD user e-mail addresses (john.smith.ctr@army.mil or john.smith.uk@army.mil); - DoD user e-mail display names (e.g., John Smith, Contractor <john.smith.ctr@army.mil> or John Smith, United Kingdom <john.smith.uk@army.mil>); and - automated signature blocks (e.g., John Smith, Contractor, J-6K, Joint Staff or John Doe, Australia, LNO, Combatant Command). Contractors who are also foreign nationals are identified as both, e.g., john.smith.ctr.uk@army.mil. DoD has defined the characteristics as contractor or government employee and by nationality. User identifiers will follow the same format as DoD user e-mail addresses (john.smith.ctr@army.mil or john.smith.uk@army.mil);	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed manages individual identifiers by uniquely identifying each individual as contractor or government employee and by nationality. User identifiers will follow the same format as DoD user e-mail addresses (john.smith.ctr@army.mil or john.smith.uk@army.mil); - DoD user e-mail display names (e.g., John Smith, Contractor <john.smith.ctr@army.mil> or John Smith, United Kingdom <john.smith.uk@army.mil>); and - automated signature blocks (e.g., John Smith, Contractor, J-6K, Joint Staff or John Doe, Australia, LNO, Combatant Command). Contractors who are also foreign nationals are identified as both, e.g., john.smith.ctr.uk@army.mil. DoD has defined the characteristics as contractor or government employee and by nationality. User identifiers will follow the same format as DoD user e-mail addresses (john.smith.ctr@army.mil or john.smith.uk@army.mil); - DoD user e-mail display names (e.g., John Smith, Contractor <john.smith.ctr@army.mil> or John Smith, United Kingdom <john.smith.uk@army.mil>); and - automated signature blocks (e.g., John Smith, Contractor, J-6K, Joint Staff or John Doe, Australia,
IA-5	IA-5 (f)	CCI-000180	The organization manages information system authenticators by establishing maximum lifetime restrictions for authenticators.	Per IA-5, CCI 1610, DoD has established the maximum lifetime restrictions for authenticators as CAC - every 3 years, or 1 year from term of contract Password: 60 days Biometrics: every 3 years.	Per IA-5, CCI 1610, DoD has established the maximum lifetime restrictions for authenticators as CAC - every 3 years, or 1 year from term of contract Password: 60 days Biometrics: every 3 years.
IA-5	IA-5 (b)	CCI-000176	The organization manages information system authenticators by establishing initial authenticator content for authenticators defined by the organization.	The organization being inspected/assessed defines and documents procedures for setting initial authenticator content.	The organization conducting the inspection/assessment obtains and examines the documented procedures for setting initial authenticator content to ensure they have been defined.
IA-5	IA-5 (c)	CCI-001544	The organization manages information system authenticators by ensuring that authenticators have sufficient strength of mechanism for their intended use.	The organization being inspected/assessed documents and implements authenticator strength mechanisms sufficient for the intended use of the authenticators.	The organization conducting the inspection/assessment obtains and examines documented authenticator strength mechanisms to ensure that they are defined and that the mechanisms have sufficient strength for the intended use of the authenticators.
IA-5	IA-5 (d)	CCI-001984	The organization manages information system authenticators by establishing administrative procedures for revoking authenticators.	The organization being inspected/assessed defines and documents procedures for revoking authenticators.	The organization conducting the inspection/assessment obtains and examines the documented procedures for revoking authenticators to ensure the procedures are defined.
IA-5	IA-5 (f)	CCI-000181	The organization manages information system authenticators by establishing reuse conditions for authenticators.	The organization being inspected/assessed defines and documents the reuse conditions for authenticators.	The organization conducting the inspection/assessment obtains and examines the documented reuse conditions for authenticators to ensure they have been defined.
IA-5	IA-5 (h)	CCI-000183	The organization manages information system authenticators by protecting authenticator content from unauthorized disclosure.	The organization being inspected/assessed documents and implements procedures to protect authenticator content from unauthorized disclosure.	The organization conducting the inspection/assessment obtains and examines the documented procedures to protect authenticator content from unauthorized disclosure to ensure the procedures are defined.
IA-5	IA-5 (d)	CCI-001985	The organization manages information system authenticators by implementing administrative procedures for initial authenticator distribution.	The organization being inspected/assessed implements administrative procedures for initial authenticator distribution as documented in IA-5, CCIs 1980 & 1981.	The organization conducting the inspection/assessment obtains and examines records of initial authenticator distribution and interviews individuals responsible for authenticator distribution to ensure that the organization being inspected/assessed implements the process as defined in IA-5, CCIs 1980 & 1981.
IA-5	IA-5 (d)	CCI-001986	The organization manages information system authenticators by implementing administrative procedures for lost/compromised authenticators.	The organization being inspected/assessed implements administrative procedures for the response to lost/compromised authenticators as documented in IA-5, CCI 1982.	The organization conducting the inspection/assessment obtains and examines documented procedures for the response to lost/compromised authenticators to ensure that the organization being inspected/assessed implements the process as defined in IA-5, CCI 1982.
IA-5	IA-5 (d)	CCI-001987	The organization manages information system authenticators by implementing administrative procedures for damaged authenticators.	The organization being inspected/assessed implements administrative procedures for the response to damaged authenticators as documented in IA-5, CCI 1983.	The organization conducting the inspection/assessment obtains and examines documented procedures for the response to damaged authenticators to ensure that the organization being inspected/assessed implements the process as defined in IA-5, CCI 1983.
IA-5	IA-5 (d)	CCI-001998	The organization manages information system authenticators by implementing administrative procedures for revoking authenticators.	The organization being inspected/assessed implements administrative procedures for revoking authenticators as documented in IA-5, CCI 1984.	The organization conducting the inspection/assessment obtains and examines documented procedures for revoking authenticators to ensure that the organization being inspected/assessed implements the process as defined in IA-5, CCI 1984.
IA-5	IA-5 (d)	CCI-001982	The organization manages information system authenticators by establishing administrative procedures for lost/compromised authenticators.	The organization being inspected/assessed defines and documents procedures for lost/compromised authenticators.	The organization conducting the inspection/assessment obtains and examines the documented procedures for lost/compromised authenticators to ensure they have been defined.

IA-5	IA-5 (e)	CCI-001989	The organization manages information system authenticators by changing default content of authenticators prior to information system installation.	The organization being inspected/assessed documents and implements a procedures to change default authenticators prior to information system installation.	The organization conducting the inspection/assessment obtains and examines the documented procedures to change default authenticators to ensure the procedures are defined. The organization conducting the inspection/assessment obtains and examines a sampling of authenticator age data for default accounts to ensure that default authenticators are changed prior to installation.
IA-5	IA-5 (f)	CCI-000179	The organization manages information system authenticators by establishing minimum lifetime restrictions for authenticators.	The organization being inspected/assessed defines and documents minimum lifetime restrictions for authenticators.	The organization conducting the inspection/assessment obtains and examines the documented minimum lifetime restrictions for authenticators to ensure they have been defined.
IA-5	IA-5 (a)	CCI-001980	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.	The organization being inspected/assessed defines and documents procedures for the secure distribution of authenticators. The process shall include verification of the identify of the individual, group, role, or device receiving the authenticator.	The organization conducting the inspection/assessment obtains and examines the documented procedures for the secure distribution of authenticators to ensure they have been defined and that they include a method to verify the identify of the individual, group, role, or device receiving the authenticator.
IA-5	IA-5 (d)	CCI-001981	The organization manages information system authenticators by establishing administrative procedures for initial authenticator distribution.	The organization being inspected/assessed defines and documents procedures for the secure distribution of authenticators.	The organization conducting the inspection/assessment obtains and examines the documented procedures for the secure distribution of authenticators to ensure they have been defined.
IA-5	IA-5 (g)	CCI-000182	The organization manages information system authenticators by changing/refreshing authenticators in accordance with the organization defined time period by authenticator type.	The organization being inspected/assessed documents and implements procedures for changing/refreshing authenticators in the following time periods: CAC - every 3 years, or 1 year from term of contract Password: 60 days Biometrics: every 3 years. DoD has defined the time period as CAC - every 3 years, or 1 year from term of contract Password: 60 days Biometrics: every 3 years.	The organization conducting the inspection/assessment obtains and examines the documented procedures for authenticator change/refresh to ensure the procedures are defined. The organization conducting the inspection/assessment obtains and examines a sampling of authenticator age data to ensure that authenticators are changed or refreshed in the following time periods: CAC - every 3 years, or 1 year from term of contract Password: 60 days Biometrics: every 3 years. DoD has defined the time period as CAC - every 3 years, or 1 year from term of contract Password: 60 days Biometrics: every 3 years.
IA-5	IA-5 (g)	CCI-001610	The organization defines the time period (by authenticator type) for changing/refreshing authenticators.	DoD has defined the time period as CAC - every 3 years, or 1 year from term of contract Password: 60 days Biometrics: every 3 years.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as CAC - every 3 years, or 1 year from term of contract Password: 60 days Biometrics: every 3 years.
IA-5	IA-5 (d)	CCI-001983	The organization manages information system authenticators by establishing administrative procedures for damaged authenticators.	The organization being inspected/assessed defines and documents procedures for the secure disposal of damaged authenticators.	The organization conducting the inspection/assessment obtains and examines the documented procedures for the secure disposal of damaged authenticators to ensure they have been defined.
IA-5	IA-5 (h)	CCI-002042	The organization manages information system authenticators by protecting authenticator content from unauthorized modification.	The organization being inspected/assessed configures the information system to manage information system authenticators by protecting authenticator content from unauthorized modification. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2042.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to manage information system authenticators by protecting authenticator content from unauthorized modification. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2042.
IA-5	IA-5 (i)	CCI-002366	The organization manages information system authenticators by having devices implement specific security safeguards to protect authenticators.	The organization being inspected/assessed configures the information system to manage information system authenticators by having devices implement, specific security safeguards to protect authenticators. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2366.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to manage information system authenticators by having devices implement, specific security safeguards to protect authenticators. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2366.

IA-5	IA-5 (i)	CCI-002365	The organization manages information system authenticators by requiring individuals to take specific security safeguards to protect authenticators.	The organization being inspected/assessed documents within user agreements that individuals shall safeguard authenticators.	The organization conducting the inspection/assessment obtains and examines the user agreements of the organization being inspected/assessed to ensure that there are requirements for individuals to safeguard authenticators.
IA-5	IA-5 (j)	CCI-001990	The organization manages information system authenticators by changing authenticators for group/role accounts when membership to those accounts changes.	The organization being inspected/assessed documents and implements procedures for changing authenticators for group/role accounts when membership to those accounts changes.	The organization conducting the inspection/assessment obtains and examines the documented procedures for group/role authenticator change to ensure the procedures are defined and applied when membership to those accounts changes. The organization conducting the inspection/assessment obtains and examines a sampling of authenticator age data and documentation of personnel role changes to ensure that group/role authenticators are changed when membership changes.
IA-5 (1)	IA-5 (1) (a)	CCI-000192	The information system enforces password complexity by the minimum number of upper case characters used.	The organization being inspected/assessed configures the information system to enforce password complexity by the minimum number of upper case characters used. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 192.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to enforce password complexity by the minimum number of upper case characters used. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 192.
IA-5 (1)	IA-5 (1) (a)	CCI-000193	The information system enforces password complexity by the minimum number of lower case characters used.	The organization being inspected/assessed configures the information system to enforce password complexity by the minimum number of lower case characters used. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 193.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to enforce password complexity by the minimum number of lower case characters used. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 193.
IA-5 (1)	IA-5 (1) (a)	CCI-000194	The information system enforces password complexity by the minimum number of numeric characters used.	The organization being inspected/assessed configures the information system to enforce password complexity by the minimum number of numeric characters used. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 194.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to enforce password complexity by the minimum number of numeric characters used. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 194.
IA-5 (1)	IA-5 (1) (a)	CCI-000205	The information system enforces minimum password length.	The organization being inspected/assessed configures the information system to enforce minimum password length. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 205.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to enforce minimum password length. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 205.

IA-5 (1)	IA-5 (1) (a)	CCI-001619	The information system enforces password complexity by the minimum number of special characters used.	The organization being inspected/assessed configures the information system to enforce password complexity by the minimum number of special characters used. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1619.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to enforce password complexity by the minimum number of special characters used. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1619.
IA-5 (1)	IA-5 (1) (a)	CCI-001611	The organization defines the minimum number of special characters for password complexity enforcement.	DoD has defined the minimum number of special characters for password complexity enforcement as one special character.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the minimum number of special characters for password complexity enforcement as one special character.
IA-5 (1)	IA-5 (1) (a)	CCI-001612	The organization defines the minimum number of upper case characters for password complexity enforcement.	DoD has defined the minimum number of upper case characters for password complexity enforcement as one upper-case character.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the minimum number of upper case characters for password complexity enforcement as one upper-case character.
IA-5 (1)	IA-5 (1) (a)	CCI-001613	The organization defines the minimum number of lower case characters for password complexity enforcement.	DoD has defined the minimum number of lower case characters for password complexity enforcement as one lower-case character.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the minimum number of lower case characters for password complexity enforcement as one lower-case character.
IA-5 (1)	IA-5 (1) (a)	CCI-001614	The organization defines the minimum number of numeric characters for password complexity enforcement.	DoD has defined the minimum number of numeric characters for password complexity enforcement as one numeric character.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the minimum number of numeric characters for password complexity enforcement as one numeric character.
IA-5 (1)	IA-5 (1) (b)	CCI-000195	The information system, for password-based authentication, when new passwords are created, enforces that at least an organization-defined number of characters are changed.	The organization being inspected/assessed configures the information system to enforce that at least 50% of the minimum password length is changed. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 195. DoD has defined the minimum number of characters as 50% of the minimum password length.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to enforce that at least 50% of the minimum password length is changed. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 195. DoD has defined the minimum number of characters as 50% of the minimum password length.
IA-5 (1)	IA-5 (1) (b)	CCI-001615	The organization defines the minimum number of characters that are changed when new passwords are created.	DoD has defined the minimum number of characters as 50% of the minimum password length.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the minimum number of characters as 50% of the minimum password length.
IA-5 (1)	IA-5 (1) (c)	CCI-000196	The information system, for password-based authentication, stores only cryptographically-protected passwords.	The organization being inspected/assessed configures the information system to store only encrypted representations of passwords. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 196.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to store only encrypted representations of passwords. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 196.

IA-5 (1)	IA-5 (1) (c)	CCI-000197	The information system, for password-based authentication, transmits only cryptographically-protected passwords.	The organization being inspected/assessed configures the information system to transmit only encrypted representations of passwords. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 197.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to transmit only encrypted representations of passwords. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 197.
IA-5 (1)	IA-5 (1) (d)	CCI-000198	The information system enforces minimum password lifetime restrictions.	The organization being inspected/assessed configures the information system to enforce minimum password lifetime restrictions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 198.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to enforce minimum password lifetime restrictions. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 198.
IA-5 (1)	IA-5 (1) (d)	CCI-000199	The information system enforces maximum password lifetime restrictions.	The organization being inspected/assessed configures the information system to enforce maximum password lifetime restrictions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 199.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to enforce maximum password lifetime restrictions. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 199.
IA-5 (1)	IA-5 (1) (d)	CCI-001616	The organization defines minimum password lifetime restrictions.	DoD has defined the minimum password lifetime restrictions as 24 hours.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the minimum password lifetime restrictions as 24 hours.
IA-5 (1)	IA-5 (1) (d)	CCI-001617	The organization defines maximum password lifetime restrictions.	DoD has defined the maximum password lifetime restrictions as 60 days.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the maximum password lifetime restrictions as 60 days.
IA-5 (1)	IA-5 (1) (e)	CCI-000200	The information system prohibits password reuse for the organization defined number of generations.	The organization being inspected/assessed configures the information system to prohibit reuse for a minimum of 5 generations. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 200. DoD has defined the number of generations as a minimum of 5.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to prohibit reuse for a minimum of 5 generations. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 200. DoD has defined the number of generations as a minimum of 5.
IA-5 (1)	IA-5 (1) (e)	CCI-001618	The organization defines the number of generations for which password reuse is prohibited.	DoD has defined the number of generations as a minimum of 5.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the number of generations as a minimum of 5.
IA-5 (1)	IA-5 (1) (f)	CCI-002041	The information system allows the use of a temporary password for system logons with an immediate change to a permanent password.	The organization being inspected/assessed configures the information system to allow the use of a temporary password for system logons with an immediate change to a permanent password. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2041.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to allow the use of a temporary password for system logons with an immediate change to a permanent password. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2041.

IA-5 (4)	IA-5 (4)	CCI-001996	The organization defines the requirements required by the automated tools to determine if password authenticators are sufficiently strong.	DoD has defined the requirements as the complexity as identified in IA-5 (1) Part A.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the requirements as the complexity as identified in IA-5 (1) Part A.
IA-5 (4)	IA-5 (4)	CCI-001997	The organization employs automated tools to determine if password authenticators are sufficiently strong to satisfy organization-defined requirements.	The organization being inspected/assessed implements automated tools to check passwords strength per the complexity requirements defined in IA-5 (1) Part A.	The organization conducting the inspection/assessment examines the automated tools and inspects the configuration of the automated tools to ensure that they are implemented to check password strength per the complexity requirements defined in IA-5 (1) Part A.
IA-5 (7)	IA-5 (7)	CCI-000202	The organization ensures unencrypted static authenticators are not embedded in access scripts.	The organization being inspected/assessed documents and implements requirements that unencrypted static authenticators not be embedded in access scripts.	The organization conducting the inspection/assessment obtains and examines the requirements that unencrypted static authenticators not be embedded in access scripts to ensure the organization being inspected/assessed ensures unencrypted static authenticators are not embedded in access scripts.
IA-5 (7)	IA-5 (7)	CCI-000203	The organization ensures unencrypted static authenticators are not stored on function keys.	The organization being inspected/assessed documents and implements requirements that unencrypted static authenticators not be stored on function keys.	The organization conducting the inspection/assessment obtains and examines the requirements that unencrypted static authenticators not be stored on function keys to ensure the organization being inspected/assessed ensures unencrypted static authenticators are not stored on function keys.
IA-5 (7)	IA-5 (7)	CCI-002367	The organization ensures unencrypted static authenticators are not embedded in applications.	The organization being inspected/assessed documents and implements requirements that static authenticators are not embedded in applications.	The organization conducting the inspection/assessment obtains and examines the requirements that static authenticators are not embedded in applications to ensure the organization being inspected/assessed ensures unencrypted static authenticators are not embedded in applications.
IA-5 (8)	IA-5 (8)	CCI-000204	The organization defines the security safeguards required to manage the risk of compromise due to individuals having accounts on multiple information systems.	DoD has defined the security safeguards as policies and user training including advising users not to use the same password for any of the following: Domains of differing classification levels. More than one domain of a classification level (e.g., internal agency network and Intelink). More than one privilege level (e.g., user, administrator).	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the security safeguards as policies and user training including advising users not to use the same password for any of the following: Domains of differing classification levels. More than one domain of a classification level (e.g., internal agency network and Intelink). More than one privilege level (e.g., user, administrator).
IA-5 (8)	IA-5 (8)	CCI-001621	The organization implements organization-defined security safeguards to manage the risk of compromise due to individuals having accounts on multiple information systems.	The organization being inspected/assessed documents and implements policies and user training including advising users not to use the same password for any of the following: Domains of differing classification levels. More than one domain of a classification level (e.g., internal agency network and Intelink). More than one privilege level (e.g., user, administrator).	The organization conducting the inspection/assessment obtains and examines the documented policies as well as training records to ensure that the organization being inspected/assessed implements policies and training advising users not to use the same password for any of the following: Domains of differing classification levels. More than one domain of a classification level (e.g., internal agency network and Intelink). More than one privilege level (e.g., user, administrator).
IA-5 (11)	IA-5 (11)	CCI-002002	The organization defines the token quality requirements to be employed by the information system mechanisms for token-based authentication.	DoDI 8520.03 defines types of authentication credentials that are acceptable for authentication to different systems based on the systems' information sensitivity levels and the users' access environments. The definitions for credential strengths D, E and H found in DoDI 8520.03 Enclosure 3, Section 3 specifically deal with acceptable types of hardware PKI credentials. DoD Components are automatically compliant with this control because they are covered by the DoD-level policy, DoDI 8520.03.	DoDI 8520.03 defines types of authentication credentials that are acceptable for authentication to different systems based on the systems' information sensitivity levels and the users' access environments. The definitions for credential strengths D, E and H found in DoDI 8520.03 Enclosure 3, Section 3 specifically deal with acceptable types of hardware PKI credentials. DoD Components are automatically compliant with this control because they are covered by the DoD-level policy, DoDI 8520.03.

IA-5 (11)	IA-5 (11)	CCI-002003	The information system, for token-based authentication, employs mechanisms that satisfy organization-defined token quality requirements.	The information system performing hardware token-based authentication must be configured to accept only DoD-approved PKI credentials in accordance with DoDI 8520.02 and DoDI 8520.03. For unclassified systems, DoD-approved PKI credentials include DoD PKI credentials, External Certification Authority (ECA) PKI credentials, and DoD-approved external PKI credentials. For SIPRNet, DoD-approved PKI credentials include DoD PKI credentials and NSS PKI credentials. If the information system accepts DoD-approved external PKI credentials, the information system must be configured to accept only certificates at approved assurance levels, as represented by the Certificate Policy Object Identifiers (OIDs) asserted in the certificate. The current list of DoD-approved external PKIs and acceptable Object Identifiers (OIDs) for each approved external PKI is available at http://iase.disa.mil/pki-pke/interoperability.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured the information system to accept only DoD-approved PKI credentials in accordance with (IAW) DoDI 8520.02 and DoDI 8520.03. If the information system accepts DoD-approved external PKI credentials, the organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured the information system to accept only DoD-approved external PKI credentials that assert an approved Certificate Policy OID and reject credentials issued off of DoD-approved external PKIs that do not assert an approved OID.
IA-5 (13)	IA-5 (13)	CCI-002006	The organization defines the time period after which the use of cached authenticators are prohibited.	The organization being inspected/assessed defines and documents the time period after which the use of cached authenticators are prohibited. DoD has determined the time period is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented time period to ensure it has been defined. DoD has determined the time period is not appropriate to define at the Enterprise level.
IA-5 (13)	IA-5 (13)	CCI-002007	The information system prohibits the use of cached authenticators after an organization defined time period.	The organization being inspected/assessed configures the information system to prohibit the use of cached authenticators after an organization defined time period. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2007.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to prohibit the use of cached authenticators after an organization defined time period. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2007.
IA-5 (14)	IA-5 (14)	CCI-002008	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.	DoD trust store management requirements are defined in information system components' applicable STIGs and SRGs. All information systems are required to undergo a STIG compliance review as part of their certification and accreditation process prior to being granted an authority to operate. DoD Components are automatically compliant with this CCI because they are covered by the DoD-level STIGs and SRGs.	DoD trust store management requirements are defined in information system components' applicable STIGs and SRGs. All information systems are required to undergo a STIG compliance review as part of their certification and accreditation process prior to being granted an authority to operate. DoD Components are automatically compliant with this CCI because they are covered by the DoD-level STIGs and SRGs.
IA-6	IA-6	CCI-000206	The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	The organization being inspected/assessed configures the information system to obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 206.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 206.

IA-7	IA-7	CCI-000803	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.	The organization being inspected/assessed configures the information system to implement 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. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 803.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement 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. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 803.
IA-8	IA-8	CCI-000804	The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).	The organization being inspected/assessed configures the information system to uniquely identify and authenticate non-organizational users (or processes acting on behalf of non-organizational users). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 804.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to uniquely identify and authenticate non-organizational users (or processes acting on behalf of non-organizational users). For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 804.
IA-8 (1)	IA-8 (1)	CCI-002009	The information system accepts Personal Identity Verification (PIV) credentials from other federal agencies.	The information system performing hardware token-based authentication must be configured to accept DoD-approved external PKI PIV credentials to authenticate federal agency users in accordance with DoDI 8520.02 and DoDI 8520.03. The information system must be configured to accept only certificates at approved assurance levels, as represented by the Certificate Policy Object Identifiers (OIDs) asserted in the certificate. The current list of DoD-approved external PKIs and acceptable Object Identifiers (OIDs) for each approved external PKI is available at http://iase.disa.mil/pki-pke/interoperability. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2009.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured the information system to accept DoD-approved external PKI PIV credentials in accordance with DoDI 8520.02 and DoDI 8520.03. The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured the information system to accept only DoD-approved external PKI PIV credentials that assert an approved Certificate Policy OID and reject credentials issued off of DoD-approved external PKIs that do not assert an approved OID. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2009.
IA-8 (1)	IA-8 (1)	CCI-002010	The information system electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies.	The information system performing hardware token-based authentication must be configured to validate DoD-approved external PKI PIV credentials to authenticate federal agency users in accordance with RFC 5280. The information system must be configured to perform a revocation check as part of the certificate validation process. Revocation checking may be performed using certificate revocation lists (CRLs) published by the issuing PKI or Online Certificate Status Protocol (OCSP) services. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2010.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured the information system to validate DoD-approved external PKI PIV credentials in accordance with RFC 5280. The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured the information system to perform a revocation check as part of the certificate validation process. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2010.

IA-8 (2)	IA-8 (2)	CCI-002011	The information system accepts FICAM-approved third-party credentials.	The organization being inspected/assessed configures the information system to accept Federal Identity, Credential, and Access Management (FICAM)-approved third-party credentials. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2011. FICAM Guidance is available at http://www.idmanagement.gov.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to accept FICAM-approved third-party credentials For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2011.
IA-8 (3)	IA-8 (3)	CCI-002012	The organization defines the information systems which will employ only FICAM-approved information system components.	The organization being inspected/assessed defines and documents the information systems which will employ only Federal Identity, Credential, and Access Management (FICAM)-approved information system components. DoD has determined the information systems are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented information systems to ensure they have been defined. DoD has determined the information systems are not appropriate to define at the Enterprise level.
IA-8 (3)	IA-8 (3)	CCI-002013	The organization employs only FICAM-approved information system components in organization-defined information systems to accept third-party credentials.	The organization being inspected/assessed employs only Federal Identity, Credential, and Access Management (FICAM)-approved information system components to accept third-party credentials in information systems defined in IA-8 (3), CCI 2012. FICAM Guidance is available at http://www.idmanagement.gov.	The organization conducting the inspection/assessment obtains and examines the list of information system components in use to ensure the organization being inspected/assessed uses only FICAM-approved components in information systems defined in IA-8 (3), CCI 2012.
IA-8 (4)	IA-8 (4)	CCI-002014	The information system conforms to FICAM-issued profiles.	The organization being inspected/assessed configures the information system to conform to Federal Identity, Credential, and Access Management (FICAM)-issued profiles. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2014. FICAM Guidance is available at http://www.idmanagement.gov.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to conform to FICAM-issued profiles. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2014.
IR-1	IR-1 (a)	CCI-002776	The organization defines the personnel or roles to whom the incident response policy is disseminated.	DoD has defined the roles as all personnel identified as stakeholders in the incident response process, as well as the ISSM and ISSO.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the roles as all personnel identified as stakeholders in the incident response process, as well as the ISSM and ISSO.
IR-1	IR-1 (a)	CCI-002777	The organization defines the personnel or roles to whom the incident response procedures are disseminated.	DoD has defined the roles as all personnel identified as stakeholders in the incident response process, as well as the ISSM and ISSO.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the roles as all personnel identified as stakeholders in the incident response process, as well as the ISSM and ISSO.
IR-1	IR-1 (a) (1)	CCI-000805	The organization develops and documents an incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	CJCSI 6510.01F "Information Assurance and Support to Computer Network Defense," CJCSM 6510.01B, "Cyber Incident Handling Program," DoDD O-8530.1, and DoDI O-8530.2 meets the DoD requirements for incident response policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level with the following policies: CJCSI 6510.01F, CJCSM 6510.01B, DoDD O-8530.1, and DoDI O-8530.2.	CJCSI 6510.01F "Information Assurance and Support to Computer Network Defense," CJCSM 6510.01B, "Cyber Incident Handling Program," DoDD O-8530.1, and DoDI O-8530.2 meets the DoD requirements for incident response policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level with the following policies: CJCSI 6510.01F, CJCSM 6510.01B, DoDD O-8530.1, and DoDI O-8530.2.

IR-1	IR-1 (a) (1)	CCI-000806	The organization disseminates an incident response policy to organization-defined personnel or roles.	DoD disseminates via http://www.dtic.mil/cjcs_directives/, CJCSI 6510.01F "Information Assurance and Support to Computer Network Defense," CJCSM 6510.01B, "Cyber Incident Handling Program," DoDD O-8530.1, and DoDI O-8530.2 to all personnel identified as stakeholders in the incident response process, as well as the ISSM and ISSO. DoD Components are automatically compliant with this CCI because they are covered by the DoD level with the following policies: CJCSI 6510.01F, CJCSM 6510.01B, DoDD O-8530.1, and DoDI O-8530.2.	CJCSI 6510.01F "Information Assurance and Support to Computer Network Defense," CJCSM 6510.01B, "Cyber Incident Handling Program," DoDD O-8530.1, and DoDI O-8530.2 meet the DoD requirements for incident response policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level with the following policies: CJCSI 6510.01F, CJCSM 6510.01B, DoDD O-8530.1, and DoDI O-8530.2.
IR-1	IR-1 (a) (2)	CCI-000809	The organization develops and documents procedures to facilitate the implementation of the incident response policy and associated incident response controls.	CJCSI 6510.01F "Information Assurance and Support to Computer Network Defense," CJCSM 6510.01B, "Cyber Incident Handling Program," DoDD O-8530.1, and DoDI O-8530.2 meets the DoD requirements for incident response policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level with the following policies: CJCSI 6510.01F, CJCSM 6510.01B, DoDD O-8530.1, and DoDI O-8530.2.	CJCSI 6510.01F "Information Assurance and Support to Computer Network Defense," CJCSM 6510.01B, "Cyber Incident Handling Program," DoDD O-8530.1, and DoDI O-8530.2 meet the DoD requirements for incident response policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level with the following policies: CJCSI 6510.01F, CJCSM 6510.01B, DoDD O-8530.1, and DoDI O-8530.2.
IR-1	IR-1 (a) (2)	CCI-000810	The organization disseminates incident response procedures to organization-defined personnel or roles.	DoD disseminates via http://www.dtic.mil/cjcs_directives/, CJCSI 6510.01F "Information Assurance and Support to Computer Network Defense," CJCSM 6510.01B, "Cyber Incident Handling Program," DoDD O-8530.1, and DoDI O-8530.2 to all personnel identified as stakeholders in the incident response process, as well as the ISSM and ISSO. DoD Components are automatically compliant with this CCI because they are covered by the DoD level with the following policies: CJCSI 6510.01F, CJCSM 6510.01B, DoDD O-8530.1, and DoDI O-8530.2. DoD has defined the roles as all personnel identified as stakeholders in the incident response process, as well as the ISSM and ISSO.	CJCSI 6510.01F "Information Assurance and Support to Computer Network Defense," CJCSM 6510.01B, "Cyber Incident Handling Program," DoDD O-8530.1, and DoDI O-8530.2 meet the DoD requirements for incident response policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level with the following policies: CJCSI 6510.01F, CJCSM 6510.01B, DoDD O-8530.1, and DoDI O-8530.2. DoD has defined the roles as all personnel identified as stakeholders in the incident response process, as well as the ISSM and ISSO.
IR-1	IR-1 (b) (1)	CCI-000808	The organization defines the frequency to review and update the current incident response policy.	DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.
IR-1	IR-1 (b) (1)	CCI-000807	The organization reviews and updates the current incident response policy in accordance with organization-defined frequency.	CJCSI 6510.01F "Information Assurance and Support to Computer Network Defense," CJCSM 6510.01B, "Cyber Incident Handling Program," DoDD O-8530.1, and DoDI O-8530.2 meet the DoD requirements for incident response policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level with the following policies: CJCSI 6510.01F, CJCSM 6510.01B, DoDD O-8530.1, and DoDI O-8530.2.	CJCSI 6510.01F "Information Assurance and Support to Computer Network Defense," CJCSM 6510.01B, "Cyber Incident Handling Program," DoDD O-8530.1, and DoDI O-8530.2 meet the DoD requirements for incident response policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level with the following policies: CJCSI 6510.01F, CJCSM 6510.01B, DoDD O-8530.1, and DoDI O-8530.2.
IR-1	IR-1 (b) (2)	CCI-000812	The organization defines the frequency to review and update the current incident response procedures.	DoD has defined the frequency as reviewed annually - updated as appropriate.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as reviewed annually - updated as appropriate.

IR-1	IR-1 (b) (2)	CCI-000811	The organization reviews and updates the current incident response procedures in accordance with organization-defined frequency.	DoD (in conjunction with Joint Staff for CJCSIs) reviews and updates current incident response procedures (CJCSI 6510.01F, CJCSM 6510.01B, DoDD O-8530.1, and DoDI O-8530.2) annually. DoD Components are automatically compliant with this CCI because they are covered at the DoD level with the following policies: CJCSI 6510.01F, CJCSM 6510.01B, DoDD O-8530.1, and DoDI O-8530.2. DoD has defined the frequency as reviewed annually - updated as appropriate.	CJCSI 6510.01F "Information Assurance and Support to Computer Network Defense," CJCSM 6510.01B, "Cyber Incident Handling Program," DoDD O-8530.1, and DoDI O-8530.2 meet the DoD requirements for incident response policy and procedures. DoD Components are automatically compliant with this CCI because they are covered at the DoD level with the following policies: CJCSI 6510.01F, CJCSM 6510.01B, DoDD O-8530.1, and DoDI O-8530.2. DoD has defined the frequency as reviewed annually - updated as appropriate.
IR-2	IR-2 (a)	CCI-002778	The organization defines the time period in which information system users whom assume an incident response role or responsibility receive incident response training.	DoD has defined the time period as 30 working days.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as 30 working days.
IR-2	IR-2 (a)	CCI-000813	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.	The organization being inspected/assessed documents and implement a process to provide incident response training to information system users consistent with assigned roles and responsibilities within 30 working days of assuming an incident response role or responsibility. The organization must maintain a record of training. DoD has defined the time period as 30 working days.	The organization conducting the inspection/assessment obtains and examines the documented process as well as training records for a sampling of information system users to ensure the organization being inspected/assessed provides incident response training to information system users consistent with assigned roles and responsibilities within 30 working days of assuming an incident response role or responsibility. DoD has defined the time period as 30 working days.
IR-2	IR-2 (b)	CCI-002779	The organization provides incident response training to information system users consistent with assigned roles and responsibilities when required by information system changes.	The organization being inspected/assessed documents and implements a process to provide incident response training to information system users, other than general users, consistent with assigned roles and responsibilities when required by information system changes. For general users, DoD components are automatically compliant with the requirement based on DoDD 8570.01 requirements for IA awareness training. The organization must maintain a record of training.	The organization conducting the inspection/assessment obtains and examines the documented process as well as training records for a sampling of information system users to ensure the organization being inspected/assessed provides incident response training to information system users, other than general users, consistent with assigned roles and responsibilities when required by information system changes. For general users, DoD components are automatically compliant with the requirement based on DoDD 8570.01 requirements for IA awareness training.
IR-2	IR-2 (c)	CCI-000814	The organization provides refresher incident response training in accordance with organization-defined frequency.	The organization being inspected/assessed documents and implements a process to provide incident response training to information system users, other than general users, consistent with assigned roles and responsibilities annually. For general users, DoD components are automatically compliant with the requirement based on DoDD 8570.01 requirements for IA awareness training. The organization must maintain a record of training. DoD has defined the frequency as annually.	The organization conducting the inspection/assessment obtains and examines the documented process as well as training records for a sampling of information system users to ensure the organization being inspected/assessed provides incident response training to information system users, other than general users, consistent with assigned roles and responsibilities annually. For general users, DoD components are automatically compliant with the requirement based on DoDD 8570.01 requirements for IA awareness training. DoD has defined the frequency as annually.
IR-2	IR-2 (c)	CCI-000815	The organization defines a frequency for refresher incident response training.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.

IR-3	IR-3	CCI-000818	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.	The organization being inspected/assessed documents and implements a process to test its incident response capability for the information system at least every six months for high availability and at least annually for low/med availability using tests and as defined in the incident response plan. The organization must maintain a record of test results. DoD has defined the frequency as at least every six months for high availability and at least annually for low/med availability. DoD has defined the tests as tests as defined in the incident response plan.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of test results to ensure the organization being inspected/assessed tests its incident response capability for the information system at least every six months for high availability and at least annually for low/med availability using tests and as defined in the incident response plan. DoD has defined the frequency as at least every six months for high availability and at least annually for low/med availability. DoD has defined the tests as tests as defined in the incident response plan.
IR-3	IR-3	CCI-000819	The organization defines a frequency for incident response tests.	DoD has defined the frequency as at least every six months for high availability and at least annually for low/med availability.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as at least every six months for high availability and at least annually for low/med availability.
IR-3	IR-3	CCI-000820	The organization defines tests for incident response.	DoD has defined the tests as tests as defined in the incident response plan.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the tests as tests as defined in the incident response plan.
IR-3	IR-3	CCI-001624	The organization documents the results of incident response tests.	The organization being inspected/assessed will document the results of incident response tests.	The organization conducting the inspection/assessment obtains and examines: 1. the organization's incident response plan to identify organization's testing schedule and, 2. results of previous incident response tests to ensure the organization is documenting the results IAW their incident response plan.
IR-4	IR-4 (a)	CCI-000822	The organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.	The organization being inspected/assessed must have a documented and certified CNDSP and documented procedures for information system users and site security personnel to handle incidents until they are transferred to the responsibility of the CNDSP.	The organization conducting the inspection/assessment obtains and examines the documentation identifying the CNDSP leveraged as well as the documented procedures for incident handling to ensure that there is a certified CNDSP in use and that there are procedures implemented to handle incidents until they are transferred to the responsibility of the CNDSP.
IR-4	IR-4 (b)	CCI-000823	The organization coordinates incident handling activities with contingency planning activities.	The organization being inspected/assessed will coordinate the incident response plan (IR-8) and contingency plan (CP-2) to ensure they allow for an effective transfer of information system activity and maintain confidentiality and integrity of the contigency assets.	The organization conducting the inspection/assessment obtains and examines the incident response plan (IR-8) and contingency plan (CP-2) to ensure they allow for an effective transfer of information system activity and maintain confidentiality and integrity of the contigency assets.
IR-4	IR-4 (c)	CCI-000824	The organization incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises.	The organization being inspected/assessed will conduct after action reviews from incidents to identify lessons learned and will incorporate them into procedures, training, and testing/exercises. The organization must maintain records of after action reviews.	The organization conducting the inspection/assessment obtains and examines after action reports or meeting minutes to identify actionable lessons learned to verify that lessons learned are incorporated into the plan as changes are necessary.
IR-4	IR-4 (c)	CCI-001625	The organization implements the resulting incident handling activity changes to incident response procedures, training and testing/exercise accordingly.	The organization being inspected/assessed will follow the latest incident response plan (IR-8) that has been revised (based on IR-4, CCI-000824) and disseminated.	The organization conducting the inspection/assessment obtains and examines recent changes to the incident response plan (based on IR-4, CCI 000824) to verify that they have been disseminated and reviews the most recent after action report to ensure that changes have been followed.
IR-4 (4)	IR-4 (4)	CCI-000829	The organization correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.	The organization being inspected/assessed defines procedures to examine incident information gathered and the actual actions taken by both the individuals affected and the incident response personnel. These procedures shall be defined IAW CJCSM 6510.01B. The end goal is to achieve a top level perspective of the effectiveness of the incident response and awareness.	The organization conducting the inspection/assessment obtains and examines proof of the analysis (such as minutes from an incident response after action meeting or other similar activity) to ensure that incident information is being examined and correlated.
IR-4 (6)	IR-4 (6)	CCI-002782	The organization implements incident handling capability for insider threats.	The organization being inspected/assessed documents within their incident response plan and implements plans to respond to incidents related to insider threats.	The organization conducting the inspection/assessment obtains and examines the incident response plan as well as a sampling of incident after action reports to ensure the organization being inspected/assessed implements incident handling capability for insider threats.

IR-4 (7)	IR-4 (7)	CCI-002783	The organization coordinates incident handling capability for insider threats across organization-defined components or elements of the organization.	The organization being inspected/assessed documents within their incident response plan, the responsibilities of each element of the organization defined in IR-4 (7), CCI 2784.	The organization conducting the inspection/assessment obtains and examines the incident response plan to ensure the organization being inspected/assessed coordinates incident handling capability for insider threats across components or elements of the organization defined in IR-4 (7), CCI 2784.
IR-4 (7)	IR-4 (7)	CCI-002784	The organization defines components or elements of the organization in which incident handling capability for insider threats will be coordinated.	The organization being inspected/assessed defines and documents components or elements of the organization in which incident handling capability for insider threats will be coordinated. DoD has determined the components or elements are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented components or elements to ensure the organization being inspected/assessed defines components or elements of the organization in which incident handling capability for insider threats will be coordinated. DoD has determined the components or elements are not appropriate to define at the Enterprise level.
IR-4 (8)	IR-4 (8)	CCI-002785	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.	The organization being inspected/assessed coordinates with external organizations defined in IR-4 (8), CCI 2786 to correlate and share incident information defined in IR-4 (8), CCI 2787 to achieve a cross-organization perspective on incident awareness and more effective incident responses.	The organization conducting the inspection/assessment obtains and examines reports, meeting minutes, or other evidence that the organization being inspected/assessed is coordinating with external organizations defined in IR-4 (8), CCI 2786 to correlate and share incident information defined in IR-4 (8), CCI 2787 to achieve a cross-organization perspective on incident awareness and more effective incident responses.
IR-4 (8)	IR-4 (8)	CCI-002786	The organization defines external organizations to correlate and share organization-defined incident information.	The organization being inspected/assessed defines and documents external organizations with whom they will correlate and share organization-defined incident information. DoD has determined the external organizations are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented external organizations to ensure the organization being inspected/assessed defines external organizations to correlate and share organization-defined incident information. DoD has determined the external organizations are not appropriate to define at the Enterprise level.
IR-4 (8)	IR-4 (8)	CCI-002787	The organization defines incident information to correlate and share with organization-defined external organizations.	The organization being inspected/assessed defines and documents what incident information will be correlated and shared with each external organization defined in IR-4 (8), CCI 2786. DoD has determined the incident information is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented incident information to ensure the organization being inspected/assessed defines what incident information will be correlated and shared with each external organization defined in IR-4 (8), CCI 2786. DoD has determined the incident information is not appropriate to define at the Enterprise level.
IR-5	IR-5	CCI-000832	The organization tracks and documents information system security incidents.	The organization being inspected/assessed will document within their incident handling plan, procedures to leverage the Joint Incident Management System (JIMS). For the DoD, JIMS is the automated mechanism.	The organization conducting the inspection/assessment obtains and examines the incident handling plan to ensure that there are procedures identified to leverage the JIMS.
IR-6	IR-6 (a)	CCI-000834	The organization defines a time period for personnel to report suspected security incidents to the organizational incident response capability.	DoD has defined the time period as the timeframes specified by CJCSM 6510.01B (Table C-A-1) unless the data owner provides more restrictive guidance. If organizations decide to be more restrictive than the guidance in the CJCSM, then they should address the more restrictive response time requirements in their incident response plan.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as the timeframes specified by CJCSM 6510.01B (Table C-A-1) unless the data owner provides more restrictive guidance. The organization conducting the inspection/assessment obtains and examines the incident response plan to determine if more stringent response time requirements have been identified.
IR-6	IR-6 (a)	CCI-000835	The organization requires personnel to report suspected security incidents to the organizational incident response capability within the organization-defined time period.	The organization being inspected/assessed documents within the user agreement the requirement for all system users to report suspected security incidents to the organizational incident response capability within the timeframes specified by CJCSM 6510.01B (Table C-A-1) unless the data owner provides more restrictive guidance. DoD has defined the time period as the timeframes specified by CJCSM 6510.01B (Table C-A-1) unless the data owner provides more restrictive guidance.	The organization conducting the inspection/assessment obtains and examines the user agreement to ensure users are required to report suspected security incidents to the organizational incident response capability within the timeframes specified by CJCSM 6510.01B (Table C-A-1) unless the data owner provides more restrictive guidance. DoD has defined the time period as the timeframes specified by CJCSM 6510.01B (Table C-A-1) unless the data owner provides more restrictive guidance.

IR-6	IR-6 (b)	CCI-000836	The organization reports security incident information to organization-defined authorities.	The organization being inspected/assessed documents and implements a process to report to the appropriate CIRT/CERT (such as US-CERT, DoD CERT, IC CERT).any security incidents IAW the incident response plan (IR-8). Reporting shall be conducted IAW CJCSM 6510.01B. DoD has defined the authorities as the appropriate CIRT/CERT (such as US-CERT, DoD CERT, IC CERT).	The organization conducting the inspection/assessment obtains and examines a sample of previous security incidents to ensure the incidents were reported to the appropriate CIRT/CERT (such as US-CERT, DoD CERT, IC CERT). any security incidents IAW the incident response plan (IR-8). Reporting shall be conducted IAW CJCSM 6510.01B. DoD has defined the authorities as the appropriate CIRT/CERT (such as US-CERT, DoD CERT, IC CERT).
IR-6	IR-6 (b)	CCI-002791	The organization defines authorities to whom security incident information is reported.	DoD has defined the authorities as the appropriate CIRT/CERT (such as US-CERT, DoD CERT, IC CERT).	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the authorities as the appropriate CIRT/CERT (such as US-CERT, DoD CERT, IC CERT).
IR-6 (2)	IR-6 (2)	CCI-000838	The organization reports information system vulnerabilities associated with reported security incidents to organization-defined personnel or roles.	The organization being inspected/assessed documents and implements a process to report to personnel defined in IR-6 (2), CCI 2792 information system vulnerabilities associated with reported security incident IAW the incident response plan (IR-8). Reporting shall be conducted IAW CJCSM 6510.01B.	The organization conducting the inspection/assessment obtains and examines a sample of previous security incidents to ensure the associated vulnerabilities were reported to personnel defined in IR-6 (2), CCI 2792 IAW the incident response plan (IR-8). Reporting shall be conducted IAW CJCSM 6510.01B.
IR-6 (2)	IR-6 (2)	CCI-002792	The organization defines personnel or roles to whom information system vulnerabilities associated with reported security incident information are reported.	The organization being inspected/assessed defines and documents personnel or roles to whom information system vulnerabilities associated with reported security incident information are reported. The personnel shall be identified IAW CJCSM 6510.01B. DoD has determined the personnel are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented personnel to ensure the organization being inspected/assessed defines personnel or roles to whom information system vulnerabilities associated with reported security incident information are reported IAW CJCSM 6510.01B.
IR-7	IR-7	CCI-000839	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.	The organization being inspected/assessed will establish an incident response support service, analogous to an IT help desk, to provide advice and assistance to users for handling and reporting of security incidents.	The organization conducting the inspection/assessment will interview organizational users to determine awareness of incident response support services and quality of assistance of those services when used. If interviewing organizational users is not feasible, then review users manuals/documentation to ensures it identifies an incident response support service to contact.
IR-7 (2)	IR-7 (2) (a)	CCI-000841	The organization establishes a direct, cooperative relationship between its incident response capability and external providers of information system protection capability.	The organization being inspected/assessed must establish a formal agreement with a computer network defense service provider (CNDSP).	The organization conducting the inspection/assessment obtains and examines the formal agreement document between the organization and CNDSP to validate it is current and valid.
IR-7 (2)	IR-7 (2) (b)	CCI-000842	The organization identifies organizational incident response team members to the external providers.	The organization being inspected/assessed must provide and update the list of internal incident response team members as necessary throughout the lifecycle of the CNDSP agreement, in conjunction with the CNDSP agreement.	The organization conducting the inspection/assessment obtains and examines the list of internal incident response team members to validate it is accurate and current. Interviews with CNDSP personnel and organizational incident response team members may also be conducted.
IR-8	IR-8 (a)	CCI-002794	The organization develops an incident response plan.	The organization being inspected/assessed develops and documents an incident response plan.	The organization conducting the inspection/assessment obtains and examines the documented incident response plan to ensure the organization being inspected/assessed develops an incident response plan.
IR-8	IR-8 (a) (1)	CCI-002795	The organization's incident response plan provides the organization with a roadmap for implementing its incident response capability.	The organization being inspected/assessed defines and documents within their incident response plan, a roadmap for implementing its incident response capability.	The organization conducting the inspection/assessment obtains and examines the incident response plan to ensure the organization being inspected/assessed provides within their plan, a roadmap for implementing its incident response capability.
IR-8	IR-8 (a) (2)	CCI-002796	The organization's incident response plan describes the structure and organization of the incident response capability.	The organization being inspected/assessed defines and documents within their incident response plan, the structure and organization of the incident response capability.	The organization conducting the inspection/assessment obtains and examines the incident response plan to ensure the organization being inspected/assessed describes within their plan, the structure and organization of the incident response capability.
IR-8	IR-8 (a) (3)	CCI-002797	The organization's incident response plan provides a high-level approach for how the incident response capability fits into the overall organization.	The organization being inspected/assessed defines and documents within their incident response plan, a high-level approach for how the incident response capability fits into the overall organization.	The organization conducting the inspection/assessment obtains and examines the incident response plan to ensure the organization being inspected/assessed provides within their plan, a high-level approach for how the incident response capability fits into the overall organization.
IR-8	IR-8 (a) (4)	CCI-002798	The organization's incident response plan meets the unique requirements of the organization, which relate to mission, size, structure, and functions.	The organization being inspected/assessed will ensure their incident response plan meets the unique requirements of the organization, which relate to mission, size, structure, and functions.	The organization conducting the inspection/assessment obtains and examines the incident response plan to ensure it meets the unique requirements of the organization being inspected/assessed, which relate to mission, size, structure, and functions.

IR-8	IR-8 (a) (5)	CCI-002799	The organization's incident response plan defines reportable incidents.	The organization being inspected/assessed defines and document within their incident response plan, reportable incidents IAW CJCSM 6510.01B Table B-A-2.	The organization conducting the inspection/assessment obtains and examines the incident response plan to ensure the organization being inspected/assessed defines reportable incidents IAW CJCSM 6510.01B Table B-A-2.
IR-8	IR-8 (a) (6)	CCI-002800	The organization's incident response plan provides metrics for measuring the incident response capability within the organization.	The organization being inspected/assessed defines and documents within their incident response plan, metrics for measuring the incident response capability within the organization IAW CJCSM 6510.01B, Enclosure A.	The organization conducting the inspection/assessment obtains and examines the incident response plan to ensure the organization being inspected/assessed defines metrics for measuring the incident response capability within the organization IAW CJCSM 6510.01B, Enclosure A.
IR-8	IR-8 (a) (7)	CCI-002801	The organization's incident response plan defines the resources and management support needed to effectively maintain and mature an incident response capability.	The organization being inspected/assessed defines and documents within their incident response plan, the resources and management support needed to effectively maintain and mature an incident response capability.	The organization conducting the inspection/assessment obtains and examines the incident response plan to ensure the organization being inspected/assessed defines within their plan, the resources and management support needed to effectively maintain and mature an incident response capability.
IR-8	IR-8 (a) (8)	CCI-002802	The organization defines personnel or roles to review and approve the incident response plan.	DoD has defined the personnel or roles as at a minimum, the ISSM and ISSO.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as at a minimum, the ISSM and ISSO.
IR-8	IR-8 (a) (8)	CCI-000844	The organization develops an incident response plan that is reviewed and approved by organization-defined personnel or roles.	The organization being inspected/assessed will have an incident response plan signed and approved by at a minimum, the ISSM and ISSO. DoD has defined the personnel or roles as at a minimum, the ISSM and ISSO.	The organization conducting the inspection/assessment obtains and examines the incident response plan to validate it has been properly signed by at a minimum, the ISSM and ISSO. DoD has defined the personnel or roles as at a minimum, the ISSM and ISSO.
IR-8	IR-8 (b)	CCI-000845	The organization defines incident response personnel (identified by name and/or by role) and organizational elements to whom copies of the incident response plan is distributed.	DoD has defined the list as all stakeholders identified in the incident response plan.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the list as all stakeholders identified in the incident response plan.
IR-8	IR-8 (b)	CCI-000846	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.	The organization being inspected/assessed makes available to all stakeholders identified in the incident response plan via organizationally approved information sharing mechanism. DoD has defined the list as all stakeholders identified in the incident response plan.	The organization conducting the inspection/assessment obtains and examines organizationally approved information sharing mechanism to validate all stakeholders identified in the incident response plan have adequate access to the incident response plan. DoD has defined the list as all stakeholders identified in the incident response plan.
IR-8	IR-8 (c)	CCI-000847	The organization defines the frequency for reviewing the incident response plan.	DoD has defined the frequency as at least annually (incorporating lessons learned from past incidents).	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as at least annually (incorporating lessons learned from past incidents).
IR-8	IR-8 (c)	CCI-000848	The organization reviews the incident response plan on an organization-defined frequency.	The organization being inspected/assessed will conduct reviews of its incident response plan at least annually. DoD has defined the frequency as at least annually (incorporating lessons learned from past incidents).	The organization conducting the inspection/assessment obtains and examines the incident response plan to validate it is current and has been reviewed within the last year. DoD has defined the frequency as at least annually (incorporating lessons learned from past incidents).
IR-8	IR-8 (d)	CCI-000849	The organization updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.	The organization being inspected/assessed must update the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing and incorporate lessons learned from past incidents (IR-4a). The organization must document the update actions as an audit trail.	The organization conducting the inspection/assessment obtains and examines documentation of the update actions for the incident response plan to ensure the organization is updating the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing and incorporating lessons learned from past incidents (IR-4a).
IR-8	IR-8 (e)	CCI-002803	The organization defines incident response personnel (identified by name and/or by role) and organizational elements to whom the incident response plan changes will be communicated.	DoD has defined the incident response personnel as all stakeholders identified in the incident response plan, not later than 30 days after the change is made.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the incident response personnel as all stakeholders identified in the incident response plan, not later than 30 days after the change is made.

IR-8	IR-8 (e)	CCI-000850	The organization communicates incident response plan changes to organization-defined incident response personnel (identified by name and/or by role) and organizational elements.	The organization being inspected/assessed communicates incident response plan changes to all stakeholders identified in the incident response plan, not later than 30 days after the change is made. DoD has defined the incident response personnel as all stakeholders identified in the incident response plan, not later than 30 days after the change is made.	The organization conducting the inspection/assessment examines the incident response plan via the inspected organization's information sharing capability (e.g. portal, intranet, email, etc.) to ensure it has been communicated to all stakeholders identified in the incident response plan, not later than 30 days after the change is made. DoD has defined the incident response personnel as all stakeholders identified in the incident response plan, not later than 30 days after the change is made.
IR-8	IR-8 (f)	CCI-002804	The organization protects the incident response plan from unauthorized disclosure and modification.	The organization being inspected/assessed protects the incident response plan from unauthorized disclosure and modification.	The organization conducting the inspection/assessment obtains and examines artifacts which identify how the incident response plan is protected to ensure the organization being inspected/assessed protects the incident response plan from unauthorized disclosure and modification.
IR-9	IR-9 (a)	CCI-002805	The organization responds to information spills by identifying the specific information involved in the information system contamination.	The organization being inspected/assessed documents within their incident response plan, a process to identify the specific information involved in the information system contamination.	The organization conducting the inspection/assessment obtains and examines the incident response plan as well as after action reports of incidents to ensure that specific information involved in the information system contamination is identified.
IR-9	IR-9 (b)	CCI-002806	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.	The organization being inspected/assessed documents within their incident response plan, a process to alert at a minimum, the Originating Classification Authority (OCA), the information owner/originator, the ISSM, the activity security manager, and the responsible computer incident response center of the information spill using a method of communication not associated with the spill. DoD has defined the personnel or roles as at a minimum, the OCA, the information owner/originator, the ISSM, the activity security manager, and the responsible computer incident response center.	The organization conducting the inspection/assessment obtains and examines the incident response plan as well as after action reports of incidents to ensure that at a minimum, the OCA, the information owner/originator, the ISSM, the activity security manager, and the responsible computer incident response center were alerted of the information spill using a method of communication not associated with the spill. DoD has defined the personnel or roles as at a minimum, the OCA, the information owner/originator, the ISSM, the activity security manager, and the responsible computer incident response center.
IR-9	IR-9 (b)	CCI-002807	The organization defines personnel or roles to be alerted of the information spill using a method of communication not associated with the spill.	DoD has defined the personnel or roles as at a minimum, the OCA, the information owner/originator, the ISSM, the activity security manager, and the responsible computer incident response center.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as at a minimum, the OCA, the information owner/originator, the ISSM, the activity security manager, and the responsible computer incident response center.
IR-9	IR-9 (c)	CCI-002808	The organization responds to information spills by isolating the contaminated information system or system component.	The organization being inspected/assessed documents within their incident response plan, a process to isolate the contaminated information system or system component.	The organization conducting the inspection/assessment obtains and examines the incident response plan as well as after action reports of incidents to ensure that the organization being inspected/assessed isolates contaminated information system or system component.
IR-9	IR-9 (d)	CCI-002809	The organization responds to information spills by eradicating the information from the contaminated information system or component.	The organization being inspected/assessed documents within their incident response plan, a process to eradicate the information from the contaminated information system or component.	The organization conducting the inspection/assessment obtains and examines the incident response plan as well as after action reports of incidents to ensure that the organization being inspected/assessed eradicates the information from the contaminated information system or component.
IR-9	IR-9 (e)	CCI-002810	The organization responds to information spills by identifying other information systems or system components that may have been subsequently contaminated.	The organization being inspected/assessed documents within their incident response plan, a process to identify other information systems or system components that may have been subsequently contaminated.	The organization conducting the inspection/assessment obtains and examines the incident response plan as well as after action reports of incidents to ensure that the organization being inspected/assessed identifies other information systems or system components that may have been subsequently contaminated.
IR-9	IR-9 (f)	CCI-002811	The organization responds to information spills by performing other organization-defined actions.	The organization being inspected/assessed documents within their incident response plan, processes to perform actions defined in IR-9, CCI 2812.	The organization conducting the inspection/assessment obtains and examines the incident response plan as well as after action reports of incidents to ensure that the organization being inspected/assessed performs actions defined in IR-9, CCI 2812.

IR-9	IR-9 (f)	CCI-002812	The organization defines other actions required to respond to information spills.	The organization being inspected/assessed defines and documents additional actions to be taken in response to spillage incidents. The actions must include the following: 1)consider the information system as classified at the same level as the spilled information until the appropriate remediation processes have been executed and verified; 2) Include the investigative team members and questions identified in CNSS Instruction 1001 in investigation of the incident; 3) Protect information regarding the incident from disclosure. DoD has determined the actions are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented additional actions to ensure the organization being inspected/assessed defines other actions required to respond to information spills. DoD has determined the actions are not appropriate to define at the Enterprise level
IR-9 (1)	IR-9 (1)	CCI-002813	The organization assigns organization-defined personnel or roles with responsibility for responding to information spills.	The organization being inspected/assessed appoints personnel or roles defined in IR-9 (1), CCI 2815 as having the responsibility for responding to information spills.	The organization conducting the inspection/assessment obtains and examines appointment letters to ensure the organization being inspected/assessed appoints personnel or roles defined in IR-9 (1), CCI 2815 as having the responsibility for responding to information spills.
IR-9 (1)	IR-9 (1)	CCI-002815	The organization defines personnel or roles to whom responsibility for responding to information spills will be assigned.	The organization being inspected/assessed defines and documents personnel or roles to whom responsibility for responding to information spills will be assigned. The personnel must include the ISSO and ISSM. DoD has determined the personnel or roles are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented personnel or roles to ensure the organization being inspected/assessed defines personnel or roles to whom responsibility for responding to information spills will be assigned, which must include the ISSO and ISSM. DoD has determined the personnel or roles are not appropriate to define at the Enterprise level.
IR-9 (2)	IR-9 (2)	CCI-002816	The organization provides information spillage response training according to an organization-defined frequency.	The organization being inspected/assessed documents and implements a process to provide information spillage response training annually. The organization must maintain a record of training. DoD has defined the frequency as annually.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the training records for a sampling of incident response personnel to ensure the organization being inspected/assessed provides information spillage response training annually. DoD has defined the frequency as annually.
IR-9 (2)	IR-9 (2)	CCI-002817	The organization defines the frequency in which to provide information spillage response training.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.
IR-9 (4)	IR-9 (4)	CCI-002820	The organization employs organization-defined security safeguards for personnel exposed to information not within assigned access authorizations.	The organization being inspected/assessed documents and implements a process to employ security safeguards defined in IR-9 (4), CCI 2821 for personnel exposed to information not within assigned access authorizations.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed employs security safeguards defined in IR-9 (4), CCI 2821 for personnel exposed to information not within assigned access authorizations.
IR-9 (4)	IR-9 (4)	CCI-002821	The organization defines security safeguards to employ for personnel exposed to information not within assigned access authorizations.	The organization being inspected/assessed defines and documents security safeguards to employ for personnel exposed to information not within assigned access authorizations. DoD has determined the security safeguards are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented security safeguards to ensure the organization being inspected/assessed defines security safeguards to employ for personnel exposed to information not within assigned access authorizations. DoD has determined the security safeguards are not appropriate to define at the Enterprise level.
MA-1	MA-1 (a)	CCI-002861	The organization defines the personnel or roles to whom a system maintenance policy is disseminated.	DoD has defined the personnel or roles as the SCA, ISSO, and maintenance personnel as needed by role in maintaining the system.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as the SCA, ISSO, and maintenance personnel as needed by role in maintaining the system.
MA-1	MA-1 (a)	CCI-002862	The organization defines the personnel or roles to whom system maintenance procedures are to be disseminated.	DoD has defined the personnel or roles as the SCA, ISSO, and maintenance personnel as needed by role in maintaining the system.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as the SCA, ISSO, and maintenance personnel as needed by role in maintaining the system.

MA-1	MA-1 (a) (1)	CCI-000852	The organization develops and documents a system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	The organization being inspected/assessed develops and documents a system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	The organization conducting the inspection/assessment obtains and examines the documented maintenance policy to ensure the organization being inspected/assessed develops and documents a system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
MA-1	MA-1 (a) (1)	CCI-000853	The organization disseminates to organization-defined personnel or roles a system maintenance policy.	The organization being inspected/assessed ensures the maintenance policy is disseminated to the SCA, ISSO, and maintenance personnel as needed by role in maintaining the system. DoD has defined the personnel or roles as the SCA, ISSO, and maintenance personnel as needed by role in maintaining the system.	The organization conducting the inspection/assessment obtains and examines the maintenance policy via the inspected organization's information sharing capability (e.g. portal, intranet, email, etc.) to ensure it has been disseminated to the SCA, ISSO, and maintenance personnel as needed by role in maintaining the system. DoD has defined the personnel or roles as the SCA, ISSO, and maintenance personnel as needed by role in maintaining the system.
MA-1	MA-1 (a) (2)	CCI-000855	The organization develops and documents procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls.	The organization being inspected/assessed documents the maintenance procedures within the Security Plan. The maintenance procedures shall be developed IAW maintenance policy provided in DoDI 8500.01..	The organization conducting the inspection/assessment obtains and examines the Security Plan to ensure maintenance procedures are documented and are developed IAW maintenance policy provided in DoDI 8500.01..
MA-1	MA-1 (a) (2)	CCI-000856	The organization disseminates to organization-defined personnel or roles procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls.	The organization being inspected/assessed ensures the maintenance procedures are disseminated to the SCA, ISSO, and maintenance personnel as needed by role in maintaining the system via an information sharing capability. DoD has defined the personnel or roles as the SCA, ISSO, and maintenance personnel as needed by role in maintaining the system.	The organization conducting the inspection/assessment examines the maintenance procedures via the inspected organization's information sharing capability (e.g. portal, intranet, email, etc.) to ensure it has been disseminated to the SCA, ISSO, and maintenance personnel as needed by role in maintaining the system. DoD has defined the personnel or roles as the SCA, ISSO, and maintenance personnel as needed by role in maintaining the system.
MA-1	MA-1 (b) (1)	CCI-000851	The organization defines the frequency to review and update the current system maintenance policy.	DoD has defined the frequency as every 5 years.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every 5 years.
MA-1	MA-1 (b) (1)	CCI-000854	The organization reviews and updates the current system maintenance policy in accordance with organization-defined frequency.	The organization being inspected/assessed reviews the current system maintenance policy every 5 years and revises as necessary to comply with DoD regulations. The organization must document each occurrence of the reviews and update actions as an audit trail. DoD has defined the frequency as every 5 years.	The organization conducting the inspection/assessment obtains and examines documentation of occurrence of reviews and update actions for the maintenance policy to ensure review is occurring every 5 years and updates are made as necessary. DoD has defined the frequency as every 5 years.
MA-1	MA-1 (b) (2)	CCI-001628	The organization defines a frequency to review and update the current system maintenance procedures.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.
MA-1	MA-1 (b) (2)	CCI-000857	The organization reviews and updates the current system maintenance procedures in accordance with organization-defined frequency.	The organization being inspected/assessed reviews the current system maintenance procedures annually and revises as needed to comply with DoD regulations. The organization must document each occurrence of the reviews and update actions as an audit trail. DoD has defined the frequency as annually.	The organization conducting the inspection/assessment obtains and examines documentation of occurrence of reviews and update actions for the maintenance procedures to ensure annual review and necessary updates are occurring. DoD has defined the frequency as annually.
MA-2	MA-2 (a)	CCI-002870	The organization schedules repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements	The organization being inspected/assessed schedules repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements. The organization must maintain a record of repairs.	The organization conducting the inspection/assessment obtains and examines the record of repairs to ensure the organization being inspected/assessed schedules repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.

MA-2	MA-2 (a)	CCI-002866	The organization schedules maintenance on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.	The organization being inspected/assessed schedules maintenance on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements. The organization must maintain a record of maintenance.	The organization conducting the inspection/assessment obtains and examines the record of maintenance to ensure the organization being inspected/assessed schedules maintenance on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.
MA-2	MA-2 (a)	CCI-002872	The organization documents repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.	The organization being inspected/assessed documents repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.	The organization conducting the inspection/assessment obtains and examines documentation of repairs to ensure the organization being inspected/assessed documents repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.
MA-2	MA-2 (a)	CCI-002868	The organization documents maintenance on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.	The organization being inspected/assessed documents maintenance on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.	The organization conducting the inspection/assessment obtains and examines documentation of maintenance to ensure the organization being inspected/assessed documents maintenance on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.
MA-2	MA-2 (a)	CCI-002873	The organization reviews records of repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.	The organization being inspected/assessed documents and implements a process to review records of repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements. The organization must maintain a record of reviews.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of reviews to ensure the organization being inspected/assessed reviews records of repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.
MA-2	MA-2 (a)	CCI-002869	The organization reviews records of maintenance on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.	The organization being inspected/assessed documents and implements a process to review records of maintenance on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements. The organization must maintain a record of reviews.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of reviews to ensure the organization being inspected/assessed reviews records of maintenance on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.
MA-2	MA-2 (a)	CCI-002871	The organization performs repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.	The organization being inspected/assessed implements a process to perform repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements. The organization must maintain a record of repair procedures followed.	The organization conducting the inspection/assessment obtains and examines the record of repair procedures followed to ensure the organization being inspected/assessed performs repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.
MA-2	MA-2 (a)	CCI-002867	The organization performs maintenance on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.	The organization being inspected/assessed implements a process to perform maintenance on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements. The organization must maintain a record of maintenance procedures followed.	The organization conducting the inspection/assessment obtains and examines the record of maintenance procedures followed to ensure the organization being inspected/assessed performs maintenance on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.
MA-2	MA-2 (b)	CCI-000859	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.	The organization being inspected/assessed 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. The organization must maintain records of all approvals and monitoring activities.	The organization conducting the inspection/assessment obtains and examines records of all approvals and monitoring activities to ensure the organization being inspected/assessed 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.
MA-2	MA-2 (c)	CCI-002874	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.	The organization being inspected/assessed defines and documents 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. DoD has determined the personnel or roles are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented personnel or roles to ensure the organization being inspected/assessed 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. DoD has determined the personnel or roles are not appropriate to define at the Enterprise level.

MA-2	MA-2 (c)	CCI-000860	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.	The organization being inspected/assessed documents within their risk management strategy personnel or roles defined in MA-2, CCI 2874 who must explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs. The organization must maintain written records of approval for the removal of the information system or system components from organizational facilities for off-site maintenance or repairs.	The organization conducting the inspection/assessment obtains and examines: 1. the organization's risk management strategy to ensure the personnel or roles defined in MA-2, CCI 2874 have been designated to approve the removal of the information system or system components; 2. and written records of approval for the removal of the information system or system components from organizational facilities for off-site maintenance or repairs to ensure the removal is explicitly approved.
MA-2	MA-2 (d)	CCI-000861	The organization sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs.	The organization being inspected/assessed sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs IAW DoDM 5200.01-V3 for classified media and DoDM 5200.01-V4 for unclassified media. The organization must maintain written records of media sanitization.	The organization conducting the inspection/assessment obtains and examines written records of media sanitization to ensure the organization sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs.
MA-2	MA-2 (e)	CCI-000862	The organization checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.	The organization being inspected/assessed identifies and documents the impacted security controls and takes steps to verify that the controls are still functioning properly following maintenance or repair actions.	The organization conducting the inspection/assessment obtains and examines documented evidence of the verification of security controls following maintenance and repair actions to ensure that the organization being inspected/assessed checks all potentially impacted security controls to verify that they are still functioning properly.
MA-2	MA-2 (f)	CCI-002876	The organization defines the maintenance-related information to include in organizational maintenance records.	The organization being inspected/assessed defines and documents the maintenance-related information to include in organizational maintenance records. DoD has determined the maintenance-related information is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented maintenance-related information to ensure the organization being inspected/assessed defines the maintenance-related information to include in organizational maintenance records. DoD has determined the maintenance-related information is not appropriate to define at the Enterprise level.
MA-2	MA-2 (f)	CCI-002875	The organization includes organization-defined maintenance-related information in organizational maintenance records.	The organization being inspected/assessed includes maintenance-related information defined in MA-2, CCI 2876 in organizational maintenance records.	The organization conducting the inspection/assessment obtains and examines maintenance records to ensure they include maintenance-related information defined in MA-2, CCI 2876.
MA-3	MA-3	CCI-000865	The organization approves information system maintenance tools.	The organization being inspected/assessed documents the approved maintenance tools within the Security Plan.	The organization conducting the inspection/assessment: 1. obtains and examines the Security Plan to ensure the list of approved maintenance tools is documented; 2. ensures only the approved maintenance tools are used within the system.
MA-3	MA-3	CCI-000866	The organization controls information system maintenance tools.	The organization being inspected/assessed controls information system maintenance tools that are approved IAW MA-3, CCI 865.	The organization conducting the inspection/assessment: 1. obtains and examines the Security Plan to identify the list of approved maintenance tools; 2. ensures the organization being inspected/assessed controls the approved information system maintenance tools.
MA-3	MA-3	CCI-000867	The organization monitors information system maintenance tools.	The organization being inspected/assessed develops and implements procedures to monitor the use of the approved information system maintenance tools IAW MA-3, CCI 865. Records of monitoring activity must be maintained.	The organization conducting the inspection/assessment obtains and examines: 1. the Security Plan to identify the list of approved maintenance tools; and 2. documented procedures to identify how the use of maintenance tools is monitored; and 3. reviews evidence that the monitoring is conducted IAW the documented procedures.
MA-3 (2)	MA-3 (2)	CCI-000870	The organization checks media containing diagnostic and test programs for malicious code before the media are used in the information system.	The organization being inspected/assessed: 1. documents and implements procedures to check all media containing diagnostic and test programs for malicious code before the media are used in the information system; and 2. Runs an automated tool set to check all media containing diagnostic and test programs for malicious code before the media are used in the information system. The organization must maintain configuration files for the automated tool set and audit logs of the tool set used to check media.	The organization conducting the inspection/assessment obtains and examines the procedures for checking all diagnostic and test media for malicious code, and a sampling of configuration files and audit logs of the tool set used to check media. The purpose of the review is to ensure the organization being inspected/assessed checks all media containing diagnostic and test programs for malicious code before the media are used in the information system.

MA-3 (3)	MA-3 (3) (a)	CCI-000871	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.	The organization being inspected/assessed documents and implements a process to take one of the following actions before authorizing removal of information equipment from the facility: 1. verify there is no organizational information contained on maintenance equipment; 2. Sanitize or destroy the equipment; 3. Retain the equipment within the facility; or 4. Obtain an exemption from personnel or roles defined in MA-3 (3), CCI 2882 explicitly authorizing removal of the equipment from the facility. The organization must maintain a record of maintenance equipment removal and actions taken.	The organization conducting the inspection/assessment obtains and examines the documented process and record of maintenance equipment removal to ensure the organization being inspected/assessed takes one of the four actions listed in the implementation guidance.
MA-3 (3)	MA-3 (3) (d)	CCI-002882	The organization defines the personnel or roles who can provide an exemption that explicitly authorizes removal of equipment from the facility.	The organization being inspected/assessed defines and documents the personnel or roles who can provide an exemption that explicitly authorizes removal of equipment from the facility. DoD has determined the personnel or roles are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented personnel or roles to ensure the organization being inspected/assessed defines the personnel or roles who can provide an exemption that explicitly authorizes removal of equipment from the facility. DoD has determined the personnel or roles are not appropriate to define at the Enterprise level.
MA-4	MA-4 (a)	CCI-000873	The organization approves nonlocal maintenance and diagnostic activities.	The organization being inspected/assessed documents the procedures for approving non-local maintenance and diagnostic activities within the Security Plan. The organization must maintain records of approved non-local maintenance and diagnostic activities.	The organization conducting the inspection/assessment obtains and examines: 1. the Security Plan to ensure the procedures for approving non-local maintenance and diagnostic activities are documented; and 2. records approving non-local maintenance and diagnostic activities.
MA-4	MA-4 (a)	CCI-000874	The organization monitors nonlocal maintenance and diagnostic activities.	The organization being inspected/assessed develops and implements procedures to monitor non-local maintenance and diagnostic activities. Records of monitoring activity must be maintained.	The organization conducting the inspection/assessment obtains and examines: 1. the Security Plan to identify the authorized non-local maintenance and diagnostic activities; and 2. documented procedures to identify how the use of non-local maintenance and diagnostic activities are monitored; and 3. reviews evidence that the monitoring is conducted IAW the documented procedures.
MA-4	MA-4 (b)	CCI-000876	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.	The organization being inspected/assessed: 1. documents within the Security Plan the non-local maintenance and diagnostic tools that are allowed; and 2. allows the use of non-local maintenance and diagnostic tools IAW the tools identified in the Security Plan and MA-4, CCI 873.	The organization conducting the inspection/assessment obtains and examines: 1. the Security Plan to ensure non-local maintenance and diagnostic tools have been identified; and 2. maintenance records to ensure only those tools allowed are used IAW MA-4, CCI 873.
MA-4	MA-4 (c)	CCI-000877	The organization employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions.	The organization being inspected/assessed configures the information system to employ strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 877.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to employ strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 877.
MA-4	MA-4 (d)	CCI-000878	The organization maintains records for nonlocal maintenance and diagnostic activities.	The organization being inspected/assessed maintains records of authorized non-local maintenance and diagnostic activities.	The organization conducting the inspection/assessment obtains records of authorized non-local maintenance and diagnostic activities, and examines a sampling to verify the organization is maintaining records for all non-local maintenance and diagnostic activities.
MA-4	MA-4 (e)	CCI-000879	The organization terminates sessions and network connections when nonlocal maintenance is completed.	The organization being inspected/assessed terminates session and network connections when non-local maintenance is completed. The organization must retain audit logs of session and network connections termination for non-local maintenance.	The organization conducting the inspection/assessment obtains and examines audit logs of session and network connections termination for non-local maintenance to ensure session and network connections are terminated when non-local maintenance is completed.

MA-4 (3)	MA-4 (3) (a)	CCI-000882	The organization requires that nonlocal maintenance and diagnostic services to be performed from an information system that implements a security capability comparable to the capability implemented on the system being serviced.	The organization being inspected/assessed clearly defines in its contracts and/or service level agreements the requirement that any IS used to conduct non-local maintenance and diagnostic services will have a security level at least as high as the security level implemented on the IS being serviced. Alternatively, the organization being inspected/assessed complies with MA-4 (3) CCIs 883 and 1631.	The organization conducting the inspection/assessment obtains and examines contracts and/or service level agreements for all non-local maintenance and diagnostic services to ensure that any IS used for those services is required to have security level at least as high as the security level implemented on the IS being serviced. Alternatively, the organization conducting the inspection/assessment ensures the organization being inspected/assessed complies with MA-4 (3) CCIs 883 and 1631.
MA-4 (3)	MA-4 (3) (b)	CCI-000883	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.	The organization being inspected/assessed removes the component to be serviced from the information system and prior to non-local maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities. Alternatively, the organization being inspected/assessed complies with MA-4 (3) CCI 882.	The organization conducting the inspection/assessment obtains and examines maintenance procedures for all non-local maintenance and diagnostic services to ensure that the organization being inspected/assessed sanitizes components before removal from organizational facilities. Alternatively, the organization conducting the inspection/assessment ensures the organization being inspected/assessed complies with MA-4 (3) CCI 882.
MA-4 (3)	MA-4 (3) (b)	CCI-001631	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.	The organization being inspected/assessed sanitizes and inspects serviced components prior to reusing them on any information system. Alternatively, the organization being inspected/assessed complies with MA-4 (3) CCI 882.	The organization conducting the inspection/assessment obtains and examines maintenance procedures for all non-local maintenance and diagnostic services to ensure that the organization being inspected/assessed sanitizes and inspects serviced components prior to reusing them on any information system. Alternatively, the organization conducting the inspection/assessment ensures the organization being inspected/assessed complies with MA-4 (3) CCI 882.
MA-4 (6)	MA-4 (6)	CCI-002890	The information system implements cryptographic mechanisms to protect the integrity of nonlocal maintenance and diagnostic communications.	The organization being inspected/assessed configures the information system to implement cryptographic mechanisms to protect the integrity of nonlocal maintenance and diagnostic communications. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2890.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement cryptographic mechanisms to protect the integrity of nonlocal maintenance and diagnostic communications. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2890.
MA-4 (6)	MA-4 (6)	CCI-003123	The information system implements cryptographic mechanisms to protect the confidentiality of nonlocal maintenance and diagnostic communications.	The organization being inspected/assessed configures the information system to implement cryptographic mechanisms to protect the confidentiality of nonlocal maintenance and diagnostic communications. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 3123.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement cryptographic mechanisms to protect the confidentiality of nonlocal maintenance and diagnostic communications. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 3123.
MA-4 (7)	MA-4 (7)	CCI-002891	The information system implements remote disconnect verification at the termination of nonlocal maintenance and diagnostic sessions.	The organization being inspected/assessed configures the information system to implement remote disconnect verification at the termination of nonlocal maintenance and diagnostic sessions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2891.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement remote disconnect verification at the termination of nonlocal maintenance and diagnostic sessions. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2891.
MA-5	MA-5 (a)	CCI-000890	The organization establishes a process for maintenance personnel authorization.	The organization being inspected/assessed clearly defines, documents, and establishes a process for the authorization of maintenance personnel.	The organization conducting the inspection/assessment obtains and examines procedures addressing maintenance personnel to ensure that the organization being inspected/assessed has established processes for the authorization of maintenance personnel.

MA-5	MA-5 (a)	CCI-000891	The organization maintains a list of authorized maintenance organizations or personnel.	The organization being inspected/assessed maintains a current list of authorized maintenance organizations or personnel.	The organization conducting the inspection/assessment obtains and examines the current list of authorized maintenance organizations or personnel to ensure the organization being inspected/assessed is maintaining the list.
MA-5	MA-5 (b)	CCI-002894	The organization ensures that non-escorted personnel performing maintenance on the information system have required access authorizations.	The organization being inspected/assessed documents and implements a process to ensure that non-escorted personnel performing maintenance on the information system have required access authorizations. The organization must maintain a record of personnel performing maintenance on the information system.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of personnel performing maintenance on the information system to ensure the organization being inspected/assessed ensures that non-escorted personnel performing maintenance on the information system have required access authorizations.
MA-5	MA-5 (c)	CCI-002895	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.	The organization being inspected/assessed defines and documents organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.	The organization conducting the inspection/assessment obtains and examines documented organizational personnel to ensure the organization being inspected/assessed 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.
MP-1	MP-1 (a) (1)	CCI-002566	The organization defines personnel or roles to whom a documented media protection policy and procedures will be disseminated.	DoD has defined the personnel or roles as all users.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as all users.
MP-1	MP-1 (a) (1)	CCI-000995	The organization develops and documents a media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	DoDI 5200.01 and DoDM 5200.01 Vol. 1-4 meet the DoD requirements for media protection policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.01 and DoDM 5200.01 Vol. 1-4.	DoDI 5200.01 and DoDM 5200.01 Vol. 1-4 meet the DoD requirements for media protection policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.01 and DoDM 5200.01 Vol. 1-4.
MP-1	MP-1 (a) (1)	CCI-000996	The organization disseminates to organization-defined personnel or roles a media protection policy.	DoDI 5200.01 and DoDM 5200.01 Vol. 1-4 meet the DoD requirements for media protection policy and procedures and is disseminated to all users via http://www.dtic.mil/whs/directives/corres/ins1.html. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.01 and DoDM 5200.01 Vol. 1-4.	DoDI 5200.01 and DoDM 5200.01 Vol. 1-4 meet the DoD requirements for media protection policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.01 and DoDM 5200.01 Vol. 1-4.
MP-1	MP-1 (a) (2)	CCI-000999	The organization develops and documents procedures to facilitate the implementation of the media protection policy and associated media protection controls.	DoDI 5200.01 and DoDM 5200.01 Vol. 1-4 meet the DoD requirements for media protection policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.01 and DoDM 5200.01 Vol. 1-4.	DoDI 5200.01 and DoDM 5200.01 Vol. 1-4 meet the DoD requirements for media protection policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.01 and DoDM 5200.01 Vol. 1-4.
MP-1	MP-1 (a) (2)	CCI-001000	The organization disseminates to organization-defined personnel or roles procedures to facilitate the implementation of the media protection policy and associated media protection controls.	DoDI 5200.01 and DoDM 5200.01 Vol. 1-4 meet the DoD requirements for media protection policy and procedures and is disseminated to all users via http://www.dtic.mil/whs/directives/corres/ins1.html. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.01 and DoDM 5200.01 Vol. 1-4.	DoDI 5200.01 and DoDM 5200.01 Vol. 1-4 meet the DoD requirements for media protection policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.01 and DoDM 5200.01 Vol. 1-4.
MP-1	MP-1 (b) (1)	CCI-000998	The organization defines a frequency for reviewing and updating the current media protection policy.	DoD has defined the frequency as every 5 years reviewed annually - updated as appropriate but at least within 10 years of date of issuance.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every 5 years reviewed annually - updated as appropriate but at least within 10 years of date of issuance.
MP-1	MP-1 (b) (1)	CCI-000997	The organization reviews and updates the current media protection policy in accordance with organization-defined frequency.	DoDI 5200.01 and DoDM 5200.01 Vol. 1-4 meet the DoD requirements for media protection policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.01 and DoDM 5200.01 Vol. 1-4.	DoDI 5200.01 and DoDM 5200.01 Vol. 1-4 meet the DoD requirements for media protection policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.01 and DoDM 5200.01 Vol. 1-4.

MP-1	MP-1 (b) (2)	CCI-001002	The organization defines a frequency for reviewing and updating the current media protection procedures.	DoD has defined the frequency as annually reviewed annually - updated as appropriate.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually reviewed annually - updated as appropriate.
MP-1	MP-1 (b) (2)	CCI-001001	The organization reviews and updates the current media protection procedures in accordance with organization-defined frequency.	DoDI 5200.01 and DoDM 5200.01 Vol. 1-4 meet the DoD requirements for media protection policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.01 and DoDM 5200.01 Vol. 1-4.	DoDI 5200.01 and DoDM 5200.01 Vol. 1-4 meet the DoD requirements for media protection policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.01 and DoDM 5200.01 Vol. 1-4.
MP-2	MP-2	CCI-001003	The organization restricts access to organization-defined types of digital and/or non-digital media to organization-defined personnel or roles.	The organization being inspected/assessed restricts access to all types of digital and/or non-digital media containing information not cleared for public release to the personnel or roles defined in MP-2, CCI 1005. DoD has defined the types of digital and non-digital media as all types of digital and/or non-digital media containing information not cleared for public release.	The organization conducting the inspection/assessment interviews organizational personnel with information system media protection responsibilities to ensure the organization being inspected/assessed restricts access to all types of digital and/or non-digital media containing information not cleared for public release to the personnel or roles defined in MP-2, CCI 1005. DoD has defined the types of digital and non-digital media as all types of digital and/or non-digital media containing information not cleared for public release.
MP-2	MP-2	CCI-001004	The organization defines types of digital and/or non-digital media for which the organization restricts access.	DoD has defined the types of digital and non-digital media as all types of digital and/or non-digital media containing information not cleared for public release.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the types of digital and non-digital media as all types of digital and/or non-digital media containing information not cleared for public release.
MP-2	MP-2	CCI-001005	The organization defines personnel or roles to restrict access to organization-defined types of digital and/or non-digital media.	The organization being inspected/assessed will define and document personnel or roles to restrict access to media IAW DoD 5200.01-M, CTO 10-133, and CTO 08-001. DoD has determined the personnel or roles are not appropriate to define at the Enterprise level, but personnel must be identified IAW DoD 5200.01-M, CTO 10-133, and CTO 08-001.	The organization conducting the inspection/assessment obtains and examines the documented personnel or roles to restrict access to media to ensure the access is granted IAW DoD 5200.01-M, CTO 10-133, and CTO 08-001. DoD has determined the personnel or roles are not appropriate to define at the Enterprise level, but personnel must be identified IAW DoD 5200.01-M, CTO 10-133, and CTO 08-001.
MP-6	MP-6 (a)	CCI-001028	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.	The organization being inspected/assessed sanitizes all media prior to disposal, release out of organizational control, or release for reuse IAW DoDM 5200.01 Vol. 1-4 using techniques and procedures IAW NIST SP 800-88. DoD has defined the sanitization techniques as techniques and procedures IAW NIST SP 800-88. DoD has defined the information system media as all media.	The organization conducting the inspection/assessment obtains and examines media sanitization records, audit records, any other relevant documents or records, and sanitization tools to ensure sanitization is in compliance with DoDM 5200.01 Vol. 1-4 and uses techniques and procedures IAW NIST SP 800-88. The objective of the review is to verify the organization is sanitizing its digital and non-digital information system media prior to disposal, release for reuse, or release out of the organizational control. DoD has defined the sanitization techniques as techniques and procedures IAW NIST SP 800-88. DoD has defined the information system media as all media.
MP-6	MP-6 (a)	CCI-002578	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.	DoD has defined the information system media as all media.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the information system media as all media.
MP-6	MP-6 (a)	CCI-002579	The organization defines the sanitization techniques and procedures in accordance with applicable federal and organization standards and policies to be used to sanitize organization-defined information system media prior to disposal, release out of organizational control, or release for reuse.	DoD has defined the sanitization techniques as techniques and procedures IAW NIST SP 800-88.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the sanitization techniques as techniques and procedures IAW NIST SP 800-88.

MP-6	MP-6 (b)	CCI-002580	The organization employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.	The organization being inspected/assessed implements sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information. The organization must maintain an audit trail of sanitization actions.	The organization conducting the inspection/assessment obtains and examines the audit trail of sanitization actions to ensure the organization being inspected/assessed implements sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.
MP-7	MP-7	CCI-002581	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.	The organization being inspected/assessed defines and documents the types of information system media to restrict or prohibit on organization-defined information systems or system components using organization-defined security safeguards. DoD has determined the types of information system media are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented type of information system media to ensure the organization being inspected/assessed defines the types of information system media to restrict or prohibit on organization-defined information systems or system components using organization-defined security safeguards. DoD has determined the types of information system media are not appropriate to define at the Enterprise level.
MP-7	MP-7	CCI-002582	The organization defines the information systems or system components to restrict or prohibit the use of organization-defined types of information system media using organization-defined security safeguards.	The organization being inspected/assessed defines and documents the information systems or system components to restrict or prohibit the use of organization-defined types of information system media using organization-defined security safeguards. DoD has determined the information systems or system components are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented information systems or system components to ensure the organization being inspected/assessed defines the information systems or system components to restrict or prohibit the use of organization-defined types of information system media using organization-defined security safeguards. DoD has determined the information systems or system components are not appropriate to define at the Enterprise level.
MP-7	MP-7	CCI-002583	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.	The organization being inspected/assessed defines and documents 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. DoD has determined the security safeguards are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented security safeguards to ensure the organization being inspected/assessed 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. DoD has determined the security safeguards are not appropriate to define at the Enterprise level.
MP-7	MP-7	CCI-002584	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.	The organization being inspected/assessed documents and enforces controls for the use of media defined in MP-7, CCI 2581 on systems defined in MP-7, CCI 2582 using security safeguards defined in MP-7, CCI 2583.	The organization conducting the inspection/assessment obtains and examines the documented controls and examines information system procedures associated with the use of media to ensure the organization being inspected/assessed documents and enforces controls for the use of media defined in MP-7, CCI 2581 on systems defined in MP-7, CCI 2582 using security safeguards defined in MP-7, CCI 2583.
MP-7 (1)	MP-7 (1)	CCI-002585	The organization prohibits the use of portable storage devices in organization information systems when such devices have no identifiable owner.	The organization being inspected/assessed does not use portable storage devices in organization information systems when such devices have no identifiable owner.	The organization conducting the inspection/assessment examines a sampling of portable storage devices used in the information system to ensure that the devices have an identifiable owner.
PE-1	PE-1 (a)	CCI-002908	The organization defines the personnel or roles to whom a physical and environmental protection policy is disseminated.	DoD has defined the roles as organizational personnel with physical and environmental protection responsibilities.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the roles as organizational personnel with physical and environmental protection responsibilities.
PE-1	PE-1 (a)	CCI-002909	The organization defines the personnel or roles to whom the physical and environmental protection procedures are disseminated.	DoD has defined the roles as organizational personnel with physical and environmental protection responsibilities.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the roles as organizational personnel with physical and environmental protection responsibilities.
PE-1	PE-1 (a) (1)	CCI-000904	The organization develops and documents a physical and environment protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	DoDI 5200.08 and DoD 5200.08-R meet the requirement for Physical and Environmental Policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.08 and DoD 5200.08-R.	DoDI 5200.08 and DoD 5200.08-R meet the requirement for Physical and Environmental Policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.08 and DoD 5200.08-R.
PE-1	PE-1 (a) (1)	CCI-000905	The organization disseminates a physical and environmental protection policy to organization-defined personnel or roles.	DoD disseminates DoDI 5200.08 and DoD 5200.08-R organization-wide via the DoD Issuances website. http://www.dtic.mil/whs/directives/corres/dir.html DoD has defined the personnel or roles as organizational personnel with physical and environmental protection responsibilities.	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 5200.08 and DoD 5200.08-R DoD has defined the personnel or roles as organizational personnel with physical and environmental protection responsibilities.

PE-1	PE-1 (a) (2)	CCI-000908	The organization develops and documents procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.	DoDI 5200.08 and DoD 5200.08-R meet the requirement for Physical and Environmental Policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.08 and DoD 5200.08-R.	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.08 and DoD 5200.08-R.
PE-1	PE-1 (a) (2)	CCI-000909	The organization disseminates physical and environmental protection procedures to organization-defined personnel or roles.	DoD disseminates DoDI 5200.08 and DoD 5200.08-R organization-wide via the DoD Issuances website. http://www.dtic.mil/whs/directives/corres/dir.html DoD has defined the personnel or roles as organizational personnel with physical and environmental protection responsibilities.	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 5200.08 and DoD 5200.08-R DoD has defined the personnel or roles as organizational personnel with physical and environmental protection responsibilities.
PE-1	PE-1 (b) (1)	CCI-000907	The organization defines the frequency to review and update the physical and environmental protection policy.	DoD has defined the frequency reviewed annually - updated as appropriate but at least within 10 years of date of issuance.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency reviewed annually - updated as appropriate but at least within 10 years of date of issuance.
PE-1	PE-1 (b) (1)	CCI-000906	The organization reviews and updates the current physical and environmental protection policy in accordance with organization-defined frequency.	DoDI 5200.08 and DoD 5200.08-R meet the requirement for Physical and Environmental Policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.08 and DoD 5200.08-R. DoD has defined the frequency reviewed annually - updated as appropriate but at least within 10 years of date of issuance.	DoDI 5200.08 and DoD 5200.08-R meet the requirement for Physical and Environmental Policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.08 and DoD 5200.08-R. DoD has defined the frequency reviewed annually - updated as appropriate but at least within 10 years of date of issuance.
PE-1	PE-1 (b) (2)	CCI-000911	The organization defines the frequency to review and update the physical and environmental protection procedures.	DoD has defined the frequency reviewed annually - updated as appropriate.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency reviewed annually - updated as appropriate.
PE-1	PE-1 (b) (2)	CCI-000910	The organization reviews and updates the current physical and environmental protection procedures in accordance with organization-defined frequency.	DoDI 5200.08 and DoD 5200.08-R meet the requirement for Physical and Environmental Policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.08 and DoD 5200.08-R. DoD has defined the frequency reviewed annually - updated as appropriate.	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.08 and DoD 5200.08-R. DoD has defined the frequency reviewed annually - updated as appropriate.
PE-2	PE-2 (a)	CCI-000912	The organization develops a list of individuals with authorized access to the facility where the information system resides.	The organization being inspected/assessed will develop and maintain a list of personnel with authorized access to the facilities where information systems reside. The organization will also take action to identify and officially designate its publicly accessible areas where access authorization is not required.	The organization conducting the inspection/assessment obtains and examines the list of personnel with authorized access to facilities where information systems reside to ensure it is current within every 90 days. The review process should also determine if the organization has identified and officially designated its publicly accessible areas where access authorization is not required. DoD has defined the frequency as every 90 days.
PE-2	PE-2 (a)	CCI-002910	The organization approves a list of individuals with authorized access to the facility where the information system resides.	The organization being inspected/assessed formally approves a list of individuals currently authorized to access the facility where the information system resides.	The organization conducting the inspection/assessment obtains and examines the list of individuals currently authorized to access the facility where the information system resides and ensures it is formally approved.
PE-2	PE-2 (a)	CCI-002911	The organization maintains a list of individuals with authorized access to the facility where the information system resides.	The organization being inspected/assessed maintains a list of individuals currently authorized to access the facility where the information system resides.	The organization conducting the inspection/assessment obtains and examines the list of individuals to ensure the organization being inspected/assessed maintains a list of individuals currently authorized to access the facility where the information system resides.
PE-2	PE-2 (b)	CCI-000913	The organization issues authorization credentials for facility access.	The organization being inspected/assessed utilizes the list of personnel with authorized access (IAW PE-2, CCI-000912) and issues credentials accordingly. The organization must document the credential issuing activity as an audit trail.	The organization conducting the inspection/assessment obtains and examines documentation of credential issuing activities to ensure credentials are issued to personnel with authorized access.

PE-2	PE-2 (c)	CCI-000914	The organization reviews the access list detailing authorized facility access by individuals in accordance with organization-defined frequency.	The organization being inspected/assessed will review the access list and authorization credentials every 90 days and document these review and approval actions as an audit trail. DoD has defined the frequency as every 90 days.	The organization conducting the inspection/assessment obtains and examines the audit records of the review actions to ensure that reviews are conducted every 90 days. DoD has defined the frequency as every 90 days.
PE-2	PE-2 (c)	CCI-000915	The organization defines the frequency to review the access list detailing authorized facility access by individuals.	DoD has defined the frequency as every 90 days.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every 90 days.
PE-2	PE-2 (c)	CCI-001635	The organization removes individuals from the facility access list when access is no longer required.	The organization being inspected/assessed will remove personnel from the authorized access list who no longer have approved access and revoke their credentials, as identified in actions per PE-2, CCI 914. The organization must document each removal and revocation action as an audit trail.	The organization conducting the inspection/assessment obtains and examines the review and approval actions documentation to ensure that personnel no longer requiring access have been removed from the authorized access list and their credentials have been revoked.
PE-3	PE-3 (a)	CCI-002915	The organization defines the entry/exit points to the facility where the information system resides.	The organization being inspected/assessed defines and documents the entry/exit points to the facility where the information system resides. DoD has determined the entry/exit points are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented entry/exit points and inspects the facility to ensure that all entry/exit points are documented. DoD has determined the entry/exit points are not appropriate to define at the Enterprise level.
PE-3	PE-3 (a)	CCI-000919	The organization enforces physical access authorizations at organization-defined entry/exit points to the facility where the information system resides.	The organization being inspected/assessed will implement physical access authorizations at entry/exit points defined in PE-3, CCI 2915 and secure those physical access points (i.e. doors and/or windows) that are not intended for normal access.	The organization conducting the inspection/assessment performs a physical inspection of facility entry/exit points defined in PE-3, CCI 2915 to ensure that either physical access authorization controls are in place for those access points considered normal access points or are properly secured. Physical access points that are not documented or are not secured would be a failure of this control.
PE-3	PE-3 (a) (1)	CCI-000920	The organization verifies individual access authorizations before granting access to the facility.	The organization being inspected/assessed verifies and grants access to facilities based upon individual access authorizations.	The organization conducting the inspection/assessment obtains and examines the access authorization list of personnel that have access to the facility (per access list implemented through PE-2, CCI 000912) where the information system resides. Inspect selected facilities to confirm the inspected organization is granting access at all physical access points to only authorized personnel.
PE-3	PE-3 (a) (2)	CCI-002916	The organization defines the physical access control systems/devices or guards that control ingress/egress to the facility.	The organization being inspected/assessed defines and documents the physical access control systems/devices or guards that control ingress/egress to the facility. DoD has determined the physical access control systems/devices are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented physical access control systems/devices to ensure the organization being inspected/assessed defines the physical access control systems/devices or guards that control ingress/egress to the facility. DoD has determined the physical access control systems/devices are not appropriate to define at the Enterprise level.
PE-3	PE-3 (a) (2)	CCI-000921	The organization controls ingress/egress to the facility using one or more organization-defined physical access control systems/devices or guards.	The organization being inspected/assessed will control ingress/egress to the facility using the physical access control devices and/or guards defined in PE-3, CCI 2916.	The organization conducting the inspection/assessment obtains and examines the list of physical access control devices and/or guards in use defined in PE-3, CCI 2916 and conducts random inspections of entry points. The purpose is to determine whether the organization is using those physical access devices and/or guards to control entry of personnel into the facility hosting the information system.
PE-3	PE-3 (b)	CCI-002918	The organization defines entry/exit points that require physical access audit logs be maintained.	The organization being inspected/assessed defines and documents entry/exit points that require physical access audit logs be maintained. DoD has determined the entry/exit points are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented entry/exit points to ensure the organization being inspected/assessed defines entry/exit points that require physical access audit logs be maintained. DoD has determined the entry/exit points are not appropriate to define at the Enterprise level.

PE-3	PE-3 (b)	CCI-002917	The organization maintains physical access audit logs for organization-defined entry/exit points.	The organization being inspected/assessed maintains physical access audit logs for entry/exit points defined in PE-3, CCI 2918.	The organization conducting the inspection/assessment obtains and examines the physical access audit logs and compares the logged entry with known access to those entry points to ensure the organization being inspected/assessed maintains physical access audit logs for entry/exit points defined in PE-3, CCI 2918. Instances of access that will be compared with the audit logs include, at a minimum, access as part of the inspection/assessment. Comparison of other entry/exit events required elsewhere in system documentation that would have occurred before the inspection/assessment such as daily checks and scheduled maintenance are strongly encouraged and help to establish a history of compliance/non-compliance.
PE-3	PE-3 (c)	CCI-002920	The organization defines security safeguards to control access to areas within the facility officially designated as publicly accessible.	The organization being inspected/assessed defines and documents security safeguards to control access to areas within the facility officially designated as publicly accessible. DoD has determined the security safeguards are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented security safeguards to ensure the organization being inspected/assessed defines security safeguards to control access to areas within the facility officially designated as publicly accessible. DoD has determined the security safeguards are not appropriate to define at the Enterprise level.
PE-3	PE-3 (c)	CCI-002919	The organization provides organization-defined security safeguards to control access to areas within the facility officially designated as publicly accessible.	The organization being inspected/assessed provides security safeguards defined in PE-3, CCI 2920 to control access to areas within the facility officially designated as publicly accessible. The organization must document which areas are officially designated as publicly accessible.	The organization conducting the inspection/assessment obtains and examines the documentation of areas officially designated as publicly accessible to ensure the organization being inspected/assessed provides security safeguards defined in PE-3, CCI 2920 to control access to areas within the facility officially designated as publicly accessible.
PE-3	PE-3 (d)	CCI-002922	The organization defines circumstances requiring visitor escorts.	The organization being inspected/assessed defines and documents circumstances requiring visitor escorts. DoD has determined the circumstances are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented circumstances to ensure the organization being inspected/assessed defines circumstances requiring visitor escorts. DoD has determined the circumstances are not appropriate to define at the Enterprise level.
PE-3	PE-3 (d)	CCI-002921	The organization escorts visitors during organization-defined circumstances requiring visitor escorts.	The organization being inspected/assessed documents and implements a process to escort visitors during circumstances defined in PE-3, CCI 2922 requiring visitor escorts.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed escorts visitors during circumstances defined in PE-3, CCI 2922 requiring visitor escorts.
PE-3	PE-3 (d)	CCI-002924	The organization defines circumstances requiring visitor monitoring.	The organization being inspected/assessed defines and documents circumstances requiring visitor monitoring. DoD has determined the circumstances are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented circumstances to ensure the organization being inspected/assessed defines circumstances requiring visitor monitoring. DoD has determined the circumstances are not appropriate to define at the Enterprise level.
PE-3	PE-3 (d)	CCI-002923	The organization monitors visitor activity during organization-defined circumstances requiring visitor monitoring.	The organization being inspected/assessed documents and implements a process to monitor visitor activity during circumstances defined in PE-3, CCI 2924 requiring visitor monitoring.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed monitors visitor activity during circumstances defined in PE-3, CCI 2924 requiring visitor monitoring.
PE-3	PE-3 (e)	CCI-000923	The organization secures keys, combinations, and other physical access devices.	The organization being inspected/assessed will secure as appropriate (in safes or secure containers) items used for physical access control such as keys, combinations, portable locks, etc. Fixed access control devices such as card readers, installed locks, key pads, etc. should be protected from tampering.	The organization conducting the inspection/assessment conducts physical inspections and interviews physical security/safety personnel to validate the organization has taken the proper precautions, and established the proper procedures to ensure it has adequately secured its keys, combinations, and other physical devices.
PE-3	PE-3 (f)	CCI-002925	The organization defines the physical access devices to inventory.	DoD has defined the physical access devices as minimally keys or any other physical token used to gain access.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the physical access devices as minimally keys or any other physical token used to gain access.
PE-3	PE-3 (f)	CCI-000925	The organization defines the frequency for conducting inventories of organization-defined physical access devices.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.

PE-3	PE-3 (f)	CCI-000924	The organization inventories organization-defined physical access devices every organization-defined frequency.	The organization being inspected/assessed conducts and documents an inventory of minimally keys or any other physical token used to gain access annually. Inventory documents must be retained for at least one year beyond the completion of the next inventory. DoD has defined the frequency as annually. DoD has defined the physical access devices as minimally keys or any other physical token used to gain access.	The organization conducting the inspection/assessment obtains and examines the records of inventory of minimally keys or any other physical token used to gain access to ensure the inventory is being conducted annually. DoD has defined the frequency as annually. DoD has defined the physical access devices as minimally keys or any other physical token used to gain access.
PE-3	PE-3 (g)	CCI-000927	The organization defines a frequency for changing combinations and keys.	DoD has defined the frequency as required by security relevant event.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as required by security relevant event.
PE-3	PE-3 (g)	CCI-000926	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.	The organization being inspected/assessed will document each occurrence of these change actions, with the reason for the action, as an audit trail for future reference. DoD has defined the frequency as required by security relevant events.	The organization conducting the inspection/assessment obtains and examines documentation of these change actions to validate the organization is changing its keys and combinations upon occurrence of security relevant events and when keys are lost, combinations are compromised, or individuals are transferred or terminated. DoD has defined the frequency as required by security relevant events.
PE-3 (1)	PE-3 (1)	CCI-000928	The organization enforces physical access authorizations to the information system in addition to the physical access controls for the facility at organization-defined physical spaces containing one or more components of the information system.	The organization being inspected/assessed will provide documentation of additional physical access authorizations for the facility/facilities at physical spaces containing one or more components of the information system defined in PE-3 (1), CCI 2926. The organization will ensure that these controls are separate from, and independent of, the physical access controls established for the facility.	The organization conducting the inspection/assessment obtains and examines the documented list of additional physical access authorizations for the facility/facilities at physical spaces containing one or more components of the information system. The objective of the examination is to determine if the organization is enforcing additional physical access authorizations to areas of the facility at physical spaces containing one or more components of the information system defined in PE-3 (1), CCI 2926. These controls are independent of the physical access controls established for the facility.
PE-3 (1)	PE-3 (1)	CCI-002926	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.	The organization being inspected/assessed defines and documents the physical spaces containing one or more components of the information system that require physical access authorizations and controls at the facility. DoD has determined the physical spaces are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented physical spaces to ensure the organization being inspected/assessed defines the physical spaces containing one or more components of the information system that require physical access authorizations and controls at the facility. DoD has determined the physical spaces are not appropriate to define at the Enterprise level.
PE-6	PE-6 (a)	CCI-002939	The organization monitors physical access to the facility where the information system resides to detect and respond to physical security incidents.	The organization being inspected/assessed will implement monitoring procedures to ensure physical access intrusion alarms and surveillance equipment are actively monitored to detect and respond to all physical access security incidents.	The organization conducting the inspection/assessment obtains and examines the inspected organization's monitoring procedures addressing physical access monitoring. Organizational personnel with physical access monitoring responsibilities are to be interviewed. The objective of the reviews and interviews is to validate the organization is actively monitoring its physical access intrusion alarms and surveillance equipment to detect and respond to all physical access security incidents.
PE-6	PE-6 (b)	CCI-000940	The organization defines a frequency for reviewing physical access logs.	DoD has defined the frequency as every 30 days.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every 30 days.
PE-6	PE-6 (b)	CCI-000939	The organization reviews physical access logs in accordance with organization-defined frequency.	The organization being inspected/assessed will review physical access logs every 30 days. The organization must document each occurrence the physical access log review, with results of any necessary incident analysis and action taken, as an audit trail for future reference. DoD has defined the frequency as every 30 days.	The organization conducting the inspection/assessment obtains and examines the inspected organization's physical access logs or records; physical access incident reports; and any other relevant documents or records. The purpose of the reviews is to determine if the organization is conducting reviews of the physical access logs every 30 days. DoD has defined the frequency as every 30 days.

PE-6	PE-6 (b)	CCI-002941	The organization defines events or potential indications of events requiring review of physical access logs.	The organization being inspected/assessed defines and documents events or potential indications of events requiring review of physical access logs. DoD has determined the events or potential indications of events are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented events or potential indications of events to ensure the organization being inspected/assessed defines events or potential indications of events requiring review of physical access logs. DoD has determined the events or potential indications of events are not appropriate to define at the Enterprise level.
PE-6	PE-6 (b)	CCI-002940	The organization reviews physical access logs upon occurrence of organization-defined events or potential indications of events	The organization being inspected/assessed documents and implements a process to review physical access logs upon occurrence of events or potential indications of events defined in PE-6, CCI 2941. The organization must maintain records of reviews.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the records of reviews to ensure the organization being inspected/assessed reviews physical access logs upon occurrence of events or potential indications of events defined in PE-6, CCI 2941.
PE-6	PE-6 (c)	CCI-000941	The organization coordinates results of reviews and investigations with the organizations incident response capability.	The organization being inspected/assessed will coordinate the results of reviews and investigations of physical security incidents with the organization's incident response capability (for physical security incidents).	The organization conducting the inspection/assessment obtains and examines documentation of physical security incidents to ensure coordination with the inspected organization's incident response capability occurred.
PE-8	PE-8 (a)	CCI-002952	The organization defines the time period to maintain visitor access records to the facility where the information system resides.	DoD has defined the time period as at least one year.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as at least one year.
PE-8	PE-8 (a)	CCI-000947	The organization maintains visitor access records to the facility where the information system resides for organization-defined time period.	The organization being inspected/assessed must maintain visitor access records for their facilities for at least one year. DoD has defined the time period as at least one year.	The organization conducting the inspection/assessment obtains and examines visitor access records to determine if the organization is maintaining visitor access records to the facility where the information system resides for at least one year. DoD has defined the time period as at least one year.
PE-8	PE-8 (b)	CCI-000949	The organization defines the frequency to review the visitor access records for the facility where the information system resides.	DoD has defined the frequency as every 30 days.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every 30 days.
PE-8	PE-8 (b)	CCI-000948	The organization reviews visitor access records in accordance with organization-defined frequency.	The organization being inspected/assessed conducts reviews of visitor access records every 30 days and must establish and maintain a documented audit trail within the authorization lifecycle. DoD has defined the frequency as every 30 days.	The organization conducting the inspection/assessment obtains and examines the audit documentation of visitor access record review to ensure the inspected organization is conducting reviews every 30 days. DoD has defined the frequency as every 30 days.
PE-12	PE-12	CCI-000963	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.	The organization being inspected/assessed must install and maintain automatic emergency lighting for the information system that activates in the event of a power outage or disruption and covers emergency exits and evacuation routes within the facility in compliance with established OSHA requirements.	The organization conducting the inspection/assessment conducts visual inspections and interviews physical security personnel to validate the organization is in compliance with established OSHA requirements by employing and maintaining emergency lighting for the information system, the emergency lighting activates in the event of a power outage or disruption, and it covers emergency exits and evacuation routes within the facility
PE-13	PE-13	CCI-000965	The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.	The organization being inspected/assessed must implement and maintain fire suppression and detection devices/systems for the information system that are supported by an independent energy source. An independent energy source is some source other than the primary energy source for that facility. Examples include sprinkler systems, hand held fire extinguishers, fixed fire hoses, and smoke detectors.	The organization conducting the inspection/assessment will conduct visual observation and interview organizational personnel with responsibilities for fire detection and suppression devices/systems. The purpose of the reviews and interviews is to validate the fire suppression and detection devices/systems for the information system are supported by an independent energy source.

PE-14	PE-14 (a)	CCI-000971	The organization maintains temperature and humidity levels within the facility where the information system resides at organization-defined acceptable levels.	Humidity controls are not required for general office areas where information system components may be in use and are only required where there are concentrations of information systems such as server farms, mainframes, etc. The organization being inspected/assessed must maintain temperature and where applicable humidity levels of for commercial grade information systems: 64.4 – 80.6 degrees F; 45% – 60% Relative Humidity; Dew Point 41.9 ° – 59°F; measured at the air intake inlet of the IT equipment casing; for other systems, levels within manufacturer specifications. DoD has defined the acceptable levels as for commercial grade information systems: 64.4 – 80.6 degrees F; 45% – 60% Relative Humidity; Dew Point 41.9 ° – 59°F; measured at the air intake inlet of the IT equipment casing; for other systems, levels within manufacturer specifications.	The organization conducting the inspection/assessment reviews temperature and humidity controls to validate that they are set within DoD specified guidelines. DoD has defined the acceptable levels as for commercial grade information systems: 64.4 – 80.6 degrees F; 45% – 60% Relative Humidity; Dew Point 41.9 ° – 59°F; measured at the air intake inlet of the IT equipment casing; for other systems, levels within manufacturer specifications.
PE-14	PE-14 (a)	CCI-000972	The organization defines acceptable temperature and humidity levels to be maintained within the facility where the information system resides.	DoD has defined the acceptable levels as for commercial grade information systems: 64.4 – 80.6 degrees F; 45% – 60% Relative Humidity; Dew Point 41.9 ° – 59°F; measured at the air intake inlet of the IT equipment casing; for other systems, levels within manufacturer specifications.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the acceptable levels as for commercial grade information systems: 64.4 – 80.6 degrees F; 45% – 60% Relative Humidity; Dew Point 41.9 ° – 59°F; measured at the air intake inlet of the IT equipment casing; for other systems, levels within manufacturer specifications.
PE-14	PE-14 (b)	CCI-000973	The organization monitors temperature and humidity levels in accordance with organization-defined frequency.	The organization being inspected/assessed will maintain an independent monitor device for temperature and humidity levels not located in the immediate vicinity of the controller continuously unless manufacturer specifications allow for a wide enough tolerance that control is not required. Records of monitoring must be maintained as an audit trail within the authorization lifecycle. DoD has defined the frequency as continuously unless manufacturer specifications allow for a wide enough tolerance that control is not required.	The organization conducting the inspection/assessment will visually observe the inspected organization's independent monitoring device, obtain and examine audit logs, and interview physical security/safety personnel to validate the inspected organization monitors temperature and humidity levels continuously unless manufacturer specifications allow for a wide enough tolerance that control is not required. DoD has defined the frequency as continuously unless manufacturer specifications allow for a wide enough tolerance that control is not required.
PE-14	PE-14 (b)	CCI-000974	The organization defines a frequency for monitoring temperature and humidity levels.	DoD has defined the frequency as continuously unless manufacturer specifications allow for a wide enough tolerance that control is not required.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as continuously unless manufacturer specifications allow for a wide enough tolerance that control is not required.
PE-15	PE-15	CCI-000977	The organization protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible.	The organization being inspected/assessed must provide master shutoff valves that are accessible to protect the information system from damage resulting from water leakage.	The organization conducting the inspection/assessment will inspect the master shutoff valves to ensure they are installed and accessible.
PE-15	PE-15	CCI-000978	The organization protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are working properly.	The organization being inspected/assessed will ensure that master shutoff valves are working properly and have been inspected by the appropriate organization (e.g., fire marshal, department of public works).	The organization conducting the inspection/assessment will visually inspect master shutoff valve inspection documentation (e.g., inspection form, tag attached to valve).
PE-15	PE-15	CCI-000979	Key personnel have knowledge of the master water shutoff or isolation valves.	The organization being inspected/assessed will identify and document key personnel and will provide training on the location and procedures for use of master shutoff valves.	The organization conducting the inspection/assessment obtains and examines list of key personnel with knowledge of location and activation procedures for master shutoff valves and any other relevant documents or records. Interview key personnel from the list to determine if identified key personnel within the organization have knowledge of the master shutoff valves.
PE-16	PE-16	CCI-000981	The organization authorizes organization-defined types of information system components entering and exiting the facility.	The organization being inspected/assessed authorizes and maintains authorization records of all system components entering and exiting the facility. DoD has defined the types of information system components as all system components.	The organization conducting the inspection/assessment obtains and examines records authorizing all system components entering and exiting the facility. DoD has defined the types of information system components as all system components.

PE-16	PE-16	CCI-000982	The organization monitors organization-defined types of information system components entering and exiting the facility.	The organization being inspected/assessed monitors all system components entering and exiting the facility. DoD has defined the types of information system components as all system components.	The organization conducting the inspection/assessment obtains and examines records monitoring all system components entering and exiting the facility. DoD has defined the types of information system components as all system components.
PE-16	PE-16	CCI-000983	The organization controls organization-defined types of information system components entering and exiting the facility.	The organization being inspected/assessed: 1. Documents in their physical and environmental protection plan (PE-1) controls for all system components entering and exiting the facility. 2. Implements documented controls for system components entering and exiting the facility. DoD has defined the types of information system components as all system components.	The organization conducting the inspection/assessment obtains and examines the physical and environmental protection plan to determine if controls have been documented for all system components entering and exiting the facility and visually inspects the controls (e.g., logs, scans, etc.) to ensure implementation. DoD has defined the types of information system components as all system components.
PE-16	PE-16	CCI-000984	The organization maintains records of information system components entering and exiting the facility.	The organization being inspected/assessed will maintain records of all information system components entering and exiting the facility. If the organization is following General Records Schedule (GRS) 18, Section 12 they are automatically compliant.	The organization conducting the inspection/assessment obtains and examines records of physical entry and exit events to the facility. The purpose of the reviews is to ensure the organization is maintaining detailed and accurate records of information system components that enter and exit the facility. If the organization is following GRS 18, Section 12 they are automatically compliant.
PE-16	PE-16	CCI-002974	The organization defines types of information system components to authorize, monitor, and control entering and exiting the facility and to maintain records.	DoD has defined the types of information system components as all system components.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the types of information system components as all system components.
PL-1	PL-1 (a)	CCI-003047	The organization defines the personnel or roles to whom a security planning policy is disseminated.	DoD has defined the roles as organizational personnel with planning responsibilities or information security responsibilities.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the roles as Organizational personnel with planning responsibilities or information security responsibilities.
PL-1	PL-1 (a)	CCI-003048	The organization defines the personnel or roles to whom the security planning procedures are disseminated.	DoD has defined the roles as organizational personnel with planning responsibilities or information security responsibilities.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the roles as Organizational personnel with planning responsibilities or information security responsibilities.
PL-1	PL-1 (a) (1)	CCI-000563	The organization develops and documents a security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	DoDI 8510.01 meets the requirements for a security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. DoD Components are automatically compliant with this CCI because they are covered by DoD level policy, DoDI 8510.01.	DoD Components are automatically compliant with this CCI because they are covered by DoD level policy, DoDI 8510.01.
PL-1	PL-1 (a) (1)	CCI-000564	The organization disseminates a security planning policy to organization-defined personnel or roles .	DoD disseminates DoDI 8510.01 via the DoD Issuances website (http://www.dtic.mil/whs/directives/corres/dir.html) to organizational personnel with planning responsibilities or information security responsibilities. DoD Components are automatically compliant with this CCI because they are covered by DoD level policy, DoDI 8510.01. DoD has defined the roles as organizational personnel with planning responsibilities or information security responsibilities.	DoD Components are automatically compliant with this CCI because they are covered by DoD level policy, DoDI 8510.01. DoD has defined the roles as organizational personnel with planning responsibilities or information security responsibilities.
PL-1	PL-1 (a) (2)	CCI-000566	The organization develops and documents procedures to facilitate the implementation of the security planning policy and associated security planning controls.	DoDI 8510.01 meets the requirements for developing and documenting procedures to facilitate the implementation of the security planning policy and associated security planning controls. DoD Components are automatically compliant with this CCI because they are covered by DoD level policy, DoDI 8510.01.	DoD Components are automatically compliant with this CCI because they are covered by DoD level policy, DoDI 8510.01.

PL-1	PL-1 (b) (1)	CCI-001636	The organization defines the frequency to review and update the current security planning policy.	DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.
PL-1	PL-1 (b) (1)	CCI-001637	The organization reviews and updates the current security planning policy in accordance with organization-defined frequency.	DoDI 8510.01 meets the requirements for a security planning policy. DoD Components are automatically compliant with this CCI because they are covered by DoD level policy, DoDI 8510.01. DoD has defined the frequency as every 5 years.	DoDI 8510.01 meets the requirements for a security planning policy. DoD Components are automatically compliant with this CCI because they are covered by DoD level policy, DoDI 8510.01. DoD has defined the frequency as every 5 years.
PL-1	PL-1 (b) (2)	CCI-001638	The organization defines the frequency to review and update the current security planning procedures.	DoD has defined the frequency as reviewed annually - updated as appropriate.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as reviewed annually - updated as appropriate.
PL-1	PL-1 (b) (2)	CCI-000568	The organization reviews and updates the current security planning procedures in accordance with organization-defined frequency.	DoDI 8510.01 meets the requirements for a security planning policy. DoD Components are automatically compliant with this CCI because they are covered by DoD level policy, DoDI 8510.01. DoD has defined the frequency as reviewed annually - updated as appropriate.	DoDI 8510.01 meets the requirements for a security planning policy. DoD Components are automatically compliant with this CCI because they are covered by DoD level policy, DoDI 8510.01. DoD has defined the frequency as reviewed annually - updated as appropriate.
PL-1	PL-1 (b) (2)	CCI-000567	The organization disseminates security planning procedures to organization-defined personnel or roles.	DoD disseminates DoDI 8510.01 via the DoD Issuances website (http://www.dtic.mil/whs/directives/corres/dir.html) to organizational personnel with planning responsibilities or information security responsibilities. DoD Components are automatically compliant with this CCI because they are covered by DoD level policy, DoDI 8510.01. DoD has defined the roles as organizational personnel with planning responsibilities or information security responsibilities.	DoD Components are automatically compliant with this CCI because they are covered by DoD level policy, DoDI 8510.01. DoD has defined the roles as organizational personnel with planning responsibilities or information security responsibilities.
PL-2	PL-2 (a)	CCI-003049	The organization develops a security plan for the information system.	The organization being inspected/assessed develops and documents a security plan for the information system.	The organization conducting the inspection/assessment obtains and examines the documented security plan to ensure the organization being inspected/assessed develops a security plan for the information system.
PL-2	PL-2 (a) (1)	CCI-003050	The organization's security plan for the information system is consistent with the organization's enterprise architecture.	The organization being inspected/assessed defines a security plan for the information system which is consistent with the organization's enterprise architecture.	The organization conducting the inspection/assessment obtains and examines the security plan and the enterprise architecture to ensure the organization's security plan for the information system is consistent with the organization's enterprise architecture.
PL-2	PL-2 (a) (2)	CCI-003051	The organization's security plan for the information system explicitly defines the authorization boundary for the system.	The organization being inspected/assessed explicitly defines within the security plan the authorization boundary for the system.	The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed explicitly defines within the security plan the authorization boundary for the system.
PL-2	PL-2 (a) (3)	CCI-003052	The organization's security plan for the information system describes the operational context of the information system in terms of missions and business processes.	The organization being inspected/assessed describes within the security plan the operational context of the information system in terms of missions and business processes.	The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed describes within the security plan the operational context of the information system in terms of missions and business processes.
PL-2	PL-2 (a) (4)	CCI-003053	The organization's security plan for the information system provides the security categorization of the information system including supporting rationale.	The organization being inspected/assessed defines within the security plan the security categorization of the information system including supporting rationale.	The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed defines within the security plan the security categorization of the information system including supporting rationale.
PL-2	PL-2 (a) (5)	CCI-003054	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.	The organization being inspected/assessed describes within the security plan the operational environment for the information system and relationships with or connections to other information systems.	The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed describes within the security plan the operational environment for the information system and relationships with or connections to other information systems.

PL-2	PL-2 (a) (6)	CCI-003055	The organization's security plan for the information system provides an overview of the security requirements for the system	The organization being inspected/assessed documents within the security plan, an overview of the security requirements for the system.	The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed their security plan for the information system provides an overview of the security requirements for the system
PL-2	PL-2 (a) (7)	CCI-003056	The organization's security plan for the information system identifies any relevant overlays, if applicable.	The organization being inspected/assessed identifies within the security plan any relevant overlays, if applicable.	The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed identifies within the security plan any relevant overlays, if applicable.
PL-2	PL-2 (a) (8)	CCI-003057	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.	The organization being inspected/assessed describes within the security plan the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions.	The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed describes within the security plan the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions.
PL-2	PL-2 (a) (9)	CCI-000571	The organization's security plan for the information system is reviewed and approved by the authorizing official or designated representative prior to plan implementation.	The organization being inspected/assessed obtains security plan approval by the authorizing official or designated representative prior to plan implementation.	The organization conducting the inspection/assessment obtains and examines the security plan approval to ensure the organization being inspected/assessed obtains security plan approval by the authorizing official or designated representative prior to plan implementation.
PL-2	PL-2 (b)	CCI-003059	The organization distributes copies of the security plan to organization-defined personnel or roles.	The organization being inspected/assessed distributes copies of the security plan to, at a minimum, the ISSO, ISSM and SCA via the organization's information sharing portal. DoD has defined the personnel or roles as at a minimum, the ISSO, ISSM and SCA.	The organization conducting the inspection/assessment obtains and examines the security plan via the organization's information sharing portal to ensure the organization being inspected/assessed distributes copies of the security plan to at a minimum, the ISSO, ISSM and SCA via the organization's information sharing portal. DoD has defined the personnel or roles as at a minimum, the ISSO, ISSM and SCA.
PL-2	PL-2 (b)	CCI-003060	The organization defines the personnel or roles to whom copies of the security plan is distributed.	DoD has defined the personnel or roles as at a minimum, the ISSO, ISSM and SCA.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as at a minimum, the ISSO, ISSM and SCA.
PL-2	PL-2 (b)	CCI-003061	The organization communicates subsequent changes to the security plan to organization-defined personnel or roles.	The organization being inspected/assessed distributes changes to the security plan to, at a minimum, the ISSO, ISSM and SCA via the organization's information sharing portal. DoD has defined the personnel or roles as at a minimum, the ISSO, ISSM and SCA.	The organization conducting the inspection/assessment examines the organization's information sharing portal to ensure at a minimum, the ISSO, ISSM and SCA have been provided changes to the security plan. DoD has defined the personnel or roles as at a minimum, the ISSO, ISSM and SCA.
PL-2	PL-2 (b)	CCI-003062	The organization defines the personnel or roles to whom changes to the security plan are communicated.	DoD has defined the personnel or roles as at a minimum, the ISSO, ISSM and SCA.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as at a minimum, the ISSO, ISSM and SCA.
PL-2	PL-2 (c)	CCI-000572	The organization defines the frequency for reviewing the security plan for the information system.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.
PL-2	PL-2 (c)	CCI-000573	The organization reviews the security plan for the information system in accordance with organization-defined frequency.	The information system owner as part of the annual security control review will also review the security plan annually. Documentation of security plan reviews is required as an audit trail. DoD has defined the frequency as annually.	The organization conducting the inspection/assessment obtains and examines the audit records of security plan reviews to verify the security plan has been reviewed annually. DoD has defined the frequency as annually.
PL-2	PL-2 (d)	CCI-000574	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.	The information system owner will update the security plan as necessary to address changes to information system/environment of operation or problems identified during plan implementation or security control assessments. Documentation of security plan updates are required as an audit trail.	The organization conducting the inspection/assessment obtains and examines the audit records of security plan updates to verify the security plan is current. The purpose of the reviews is to validate the organization is updating the Information System (IS) security plan to address changes to the IS, its environment of operation, or problems identified during plan implementation or security control assessments.
PL-2	PL-2 (e)	CCI-003063	The organization protects the security plan from unauthorized disclosure.	The organization being inspected/assessed documents and implements a process to protect the security plan from unauthorized disclosure.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed protects the security plan from unauthorized disclosure.

PL-2	PL-2 (e)	CCI-003064	The organization protects the security plan from unauthorized modification.	The organization being inspected/assessed documents and implements a process to protect the security plan from unauthorized modification.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed protects the security plan from unauthorized modification.
PL-4	PL-4 (a)	CCI-000592	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.	The organization being inspected/assessed must develop and document rules that describe information system user responsibilities and expected behavior with regard to information and information system usage, acceptable use policy (AUP). Organizations should reference Joint Ethics Regulations (DoD 5500.7-R) when developing this policy.	The organization conducting the inspection/assessment obtains and examines the organization's AUP to ensure the organization has clearly defined and established rules describing information system user responsibilities and expected behavior with regard to information and information system usage.
PL-4	PL-4 (a)	CCI-001639	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.	The organization being inspected/assessed must disseminate to all information system users, via an information sharing capability, rules that describe information system user responsibilities and expected behavior with regard to information and information system usage, acceptable use policy (AUP). Organizations should disseminate the rules by providing to users and requiring signature of acceptance.	The organization conducting the inspection/assessment obtains and examines rules that describe information system user responsibilities via the inspected organization's information sharing capability (e.g. portal, intranet, email, etc.) to ensure it has been disseminated.
PL-4	PL-4 (b)	CCI-000593	The organization receives a signed acknowledgment from individuals requiring access the 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.	The organization being inspected/assessed will obtain signed acknowledgment (paper or electronic signature) from individuals indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.	The organization conducting the inspection/assessment obtains a list of individuals with active accounts and validates the existence of signed acknowledgements (paper or electronic signature) of the organizational AUP associated with a sampling of individuals selected from the list.
PL-4	PL-4 (c)	CCI-003069	The organization defines the frequency to review and update the rules of behavior.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.
PL-4	PL-4 (c)	CCI-003068	The organization reviews and updates the rules of behavior in accordance with organization-defined frequency.	The organization being inspected/assessed reviews and updates the rules of behavior annually. The organization must maintain an audit trail of reviews and updates. DoD has defined the frequency as annually.	The organization conducting the inspection/assessment obtains and examines the audit trail of reviews and updates to ensure the organization being inspected/assessed reviews and updates the rules of behavior annually. DoD has defined the frequency as annually.
PL-4	PL-4 (d)	CCI-003070	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.	The organization being inspected/assessed documents and implements a process to require individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised/updated. The signed acknowledgment portion of this control may be satisfied by the security awareness training and role-based security training programs conducted by organizations if such training includes rules of behavior.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed 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.
PL-8	PL-8 (a)	CCI-003072	The organization develops an information security architecture for the information system.	The organization being inspected/assessed develops and documents an information security architecture for the information system.	The organization conducting the inspection/assessment obtains and examines the documented information security architecture to ensure the organization being inspected/assessed develops an information security architecture for the information system.
PL-8	PL-8 (a) (1)	CCI-003073	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.	The organization being inspected/assessed describes within the information security architecture for the information system, the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information.	The organization conducting the inspection/assessment obtains and examines the information security architecture to ensure the organization being inspected/assessed describes within the information security architecture for the information system, the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information.
PL-8	PL-8 (a) (2)	CCI-003074	The organization's information security architecture for the information system describes how the information security architecture is integrated into and supports the enterprise architecture.	The organization being inspected/assessed describes within the information security architecture for the information system, how the information security architecture is integrated into and supports the enterprise architecture.	The organization conducting the inspection/assessment obtains and examines the information security architecture to ensure the organization being inspected/assessed describes within the information security architecture for the information system, how the information security architecture is integrated into and supports the enterprise architecture.

PL-8	PL-8 (a) (3)	CCI-003075	The organization's information security architecture for the information system describes any information security assumptions about, and dependencies on, external services.	The organization being inspected/assessed describes within the information security architecture for the information system, any information security assumptions about, and dependencies on, external services.	The organization conducting the inspection/assessment obtains and examines the information security architecture to ensure the organization being inspected/assessed describes within the information security architecture for the information system, any information security assumptions about, and dependencies on, external services.
PL-8	PL-8 (b)	CCI-003076	The organization reviews and updates the information security architecture in accordance with organization-defined frequency to reflect updates in the enterprise architecture.	The organization being inspected/assessed reviews and updates the information security architecture annually to reflect updates in the enterprise architecture. The organization must maintain an audit trail of reviews and updates. DoD has defined the frequency as annually.	The organization conducting the inspection/assessment obtains and examines the audit trail of reviews and updates to ensure the organization being inspected/assessed reviews and updates the information security architecture annually to reflect updates in the enterprise architecture. DoD has defined the frequency as annually.
PL-8	PL-8 (b)	CCI-003077	The organization defines the frequency to review and update the information system architecture.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.
PL-8	PL-8 (c)	CCI-003078	The organization ensures that planned information security architecture changes are reflected in the security plan.	The organization being inspected/assessed includes planned information security architecture changes in the security plan.	The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed includes planned information security architecture changes in the security plan.
PL-8	PL-8 (c)	CCI-003079	The organization ensures that planned information security architecture changes are reflected in the security Concept of Operations (CONOPS).	The organization being inspected/assessed includes planned information security architecture changes in the security Concept of Operations (CONOPS).	The organization conducting the inspection/assessment obtains and examines security CONOPS to ensure the organization being inspected/assessed includes planned information security architecture changes in the security CONOPS.
PL-8	PL-8 (c)	CCI-003080	The organization ensures that planned information security architecture changes are reflected in organizational procurements/acquisitions.	The organization being inspected/assessed includes planned information security architecture changes in organizational procurements/acquisitions.	The organization conducting the inspection/assessment obtains and examines a sampling of procurement materials to ensure the organization being inspected/assessed includes planned information security architecture changes in organizational procurements/acquisitions.
PL-8 (1)	PL-8 (1) (a)	CCI-003081	The organization designs its security architecture using a defense-in-depth approach that allocates organization-defined security safeguards to organization-defined locations.	The organization being inspected/assessed designs and documents its security architecture using a defense-in-depth approach that allocates security safeguards defined in PL-8 (1), CCI 3083 to locations defined in PL-8 (1), CCI 3085.	The organization conducting the inspection/assessment obtains and examines the security architecture to ensure the organization being inspected/assessed designs its security architecture using a defense-in-depth approach that allocates security safeguards defined in PL-8 (1), CCI 3083 to locations defined in PL-8 (1), CCI 3085.
PL-8 (1)	PL-8 (1) (a)	CCI-003082	The organization designs its security architecture using a defense-in-depth approach that allocates organization-defined security safeguards to organization-defined architectural layers.	The organization being inspected/assessed designs and documents its security architecture using a defense-in-depth approach that allocates security safeguards defined in PL-8 (1), CCI 3084 to architectural layers defined in PL-8 (1), CCI 3086.	The organization conducting the inspection/assessment obtains and examines the security architecture to ensure the organization being inspected/assessed designs its security architecture using a defense-in-depth approach that allocates security safeguards defined in PL-8 (1), CCI 3084 to architectural layers defined in PL-8 (1), CCI 3086.
PL-8 (1)	PL-8 (1) (a)	CCI-003083	The organization defines the security safeguards to be allocated to organization-defined locations.	The organization being inspected/assessed defines and documents the security safeguards to be allocated to organization-defined locations. DoD has determined the security safeguards are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented security safeguards to ensure the organization being inspected/assessed defines the security safeguards to be allocated to organization-defined locations. DoD has determined the security safeguards are not appropriate to define at the Enterprise level.
PL-8 (1)	PL-8 (1) (a)	CCI-003084	The organization defines the security safeguards to be allocated to organization-defined architectural layers.	The organization being inspected/assessed defines and documents the security safeguards to be allocated to organization-defined architectural layers. DoD has determined the security safeguards are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented security safeguards to ensure the organization being inspected/assessed defines the security safeguards to be allocated to organization-defined architectural layers. DoD has determined the security safeguards are not appropriate to define at the Enterprise level.
PL-8 (1)	PL-8 (1) (a)	CCI-003085	The organization defines the locations to which it allocates organization-defined security safeguards in the security architecture.	The organization being inspected/assessed defines and documents the locations to which it allocates organization-defined security safeguards in the security architecture. DoD has determined the locations are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented locations to ensure the organization being inspected/assessed defines the locations to which it allocates organization-defined security safeguards in the security architecture. DoD has determined the locations are not appropriate to define at the Enterprise level.

PL-8 (1)	PL-8 (1) (a)	CCI-003086	The organization defines the architectural layers to which it allocates organization-defined security safeguards in the security architecture.	The organization being inspected/assessed defines and documents the architectural layers to which it allocates organization-defined security safeguards in the security architecture. DoD has determined the architectural layers are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented architectural layers to ensure the organization being inspected/assessed defines the architectural layers to which it allocates organization-defined security safeguards in the security architecture. DoD has determined the architectural layers are not appropriate to define at the Enterprise level.
PL-8 (1)	PL-8 (1) (b)	CCI-003087	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.	The organization being inspected/assessed designs and documents its security architecture using a defense-in-depth approach that ensures that the allocated security safeguards operate in a coordinated and mutually reinforcing manner.	The organization conducting the inspection/assessment obtains and examines security architecture to ensure the organization being inspected/assessed 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.
PL-8 (2)	PL-8 (2)	CCI-003088	The organization requires that organization-defined security safeguards allocated to organization-defined locations and architectural layers are obtained from different suppliers.	The organization being inspected/assessed obtains from different suppliers security safeguards defined in PL-8 (1), CCIs 3083 and 3084 allocated to locations and architectural layers defined in PL-8 (1) CCIs 3085 and 3086.	The organization conducting the inspection/assessment obtains and examines procurement records to ensure that different suppliers are used to procure security safeguards defined in PL-8 (1), CCIs 3083 and 3084 allocated to locations and architectural layers defined in PL-8 (1) CCIs 3085 and 3086.
PM-1	PM-1 (a) (1)	CCI-000073	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.	DoDI 8500.01 and the Knowledge Service meet the requirement for this CCI, individual organizations and system owners must provide documentation of common control implementation in their Security Plan.	DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls they must be documented in their Security Plan.
PM-1	PM-1 (a) (1)	CCI-002985	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.	DoD disseminates DoDI 8500.01 organization-wide via the DoD Issuances website (http://www.dtic.mil/whs/directives/corres/dir.html) and the Knowledge Service is available via: https://rmfks.osd.mil. DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls they must be documented in their Security Plan.	DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls they must be documented in their Security Plan.
PM-1	PM-1 (a) (2)	CCI-001680	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.	DoDI 8500.01 and the Knowledge Service meet the requirement for this control; individual organizations and system owners must provide documentation of common control implementation in their Security Plan.	DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls they must be documented in their Security Plan.
PM-1	PM-1 (a) (2)	CCI-002986	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.	DoD disseminates DoDI 8500.01 organization-wide via the DoD Issuances website (http://www.dtic.mil/whs/directives/corres/dir.html) and the Knowledge Service is available via: https://rmfks.osd.mil. DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls they must be documented in their Security Plan.	DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls they must be documented in their Security Plan.
PM-1	PM-1 (a) (3)	CCI-002984	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).	DoDI 8500.01 and the Knowledge Service meet the requirement for this CCI; individual organizations and system owners must provide documentation of common control implementation in their Security Plan.	DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls they must be documented in their Security Plan.
PM-1	PM-1 (a) (3)	CCI-002987	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).	DoD disseminates DoDI 8500.01 organization-wide via the DoD Issuances website (http://www.dtic.mil/whs/directives/corres/dir.html) and the Knowledge Service is available via: https://rmfks.osd.mil. DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls they must be documented in their Security Plan.	DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls they must be documented in their Security Plan.

PM-1	PM-1 (a) (4)	CCI-000074	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.	DoDI 8500.01 and the Knowledge Service meet the requirement for this CCI; individual organizations and system owners must provide documentation of common control implementation in their Security Plan.	DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls they must be documented in their Security Plan.
PM-1	PM-1 (a) (4)	CCI-002988	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.	DoD disseminates DoDI 8500.01 organization-wide via the DoD Issuances website (http://www.dtic.mil/whs/directives/corres/dir.html) and the Knowledge Service is available via: https://rmfks.osd.mil. DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls they must be documented in their Security Plan.	DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls they must be documented in their Security Plan.
PM-1	PM-1 (b)	CCI-000076	The organization defines the frequency to review the organization-wide information security program plan.	DoD has defined the frequency as reviewed annually - updated as appropriate.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as reviewed annually - updated as appropriate.
PM-1	PM-1 (b)	CCI-000075	The organization reviews the organization-wide information security program plan on an organization-defined frequency.	DoDI 8500.01 and the Knowledge Service meet the requirement for this CCI; individual organizations and system owners must provide documentation of common control implementation in their Security Plan.	DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls they must be documented in their Security Plan.
PM-1	PM-1 (c)	CCI-000077	The organization updates the plan to address organizational changes and problems identified during plan implementation or security control assessments.	DoDI 8500.01 and the Knowledge Service meet the requirement for this CCI; individual organizations and system owners must provide documentation of common control implementation in their Security Plan.	DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls they must be documented in their Security Plan.
PM-1	PM-1 (d)	CCI-002989	The organization protects the information security program plan from unauthorized disclosure.	DoD documents and implements methods to protect the information security program plan from unauthorized disclosure by marking, labeling, and handling to prevent unauthorized disclosure. DoD ensures that all changes to the information security program plan are approved.	DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls they must be documented in their Security Plan.
PM-1	PM-1 (d)	CCI-002990	The organization protects the information security program plan from unauthorized modification.	DoD documents and implements methods to protect the information security program plan from unauthorized disclosure by marking, labeling, and handling to prevent unauthorized modification. DoD ensures that all changes to the information security program plan are approved.	DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls they must be documented in their Security Plan.
PM-2	PM-2	CCI-000078	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.	The Deputy DoD CIO for Cyber Security is the DoD Senior Information Security Officer (SISO), appointed in writing with the mission and resources to coordinate, develop, implement and maintain a DoD-wide information security program.	DoD organizations are automatically compliant with this control as they are covered by the appointment of the DoD SISO.
PM-3	PM-3 (a)	CCI-000080	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.	The organization being inspected/assessed documents and implements a process to ensure that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed 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.
PM-3	PM-3 (b)	CCI-000081	The organization employs a business case/Exhibit 300/Exhibit 53 to record the resources required.	The organization being inspected/assessed documents and implements a process to employ a business case/Exhibit 300/Exhibit 53 to record the resources required.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed employs a business case/Exhibit 300/Exhibit 53 to record the resources required.
PM-3	PM-3 (c)	CCI-000141	The organization ensures that information security resources are available for expenditure as planned.	The organization being inspected/assessed documents and implements a process to ensure that information security resources are available for expenditure as planned.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed ensure that information security resources are available for expenditure as planned.

PM-4	PM-4 (a) (1)	CCI-002991	The organization implements a process for ensuring that plans of action and milestones for the security program and associated organizational information systems are developed.	DoDI 8510.01 and the Knowledge Service meet the DoD requirements to develop a process for plans of action and milestones for the security program. DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8510.01 and the Knowledge Service.	DoDI 8510.01 and the Knowledge Service meet the DoD requirements to develop a process for plans of action and milestones for the security program. DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8510.01 and the Knowledge Service.
PM-4	PM-4 (a) (1)	CCI-000142	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.	DoDI 8510.01 and the Knowledge Service meet the DoD requirements to maintain a process for plans of action and milestones for the security program. DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8510.01 and the Knowledge Service.	DoDI 8510.01 and the Knowledge Service meet the DoD requirements to maintain a process for plans of action and milestones for the security program. DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8510.01 and the Knowledge Service.
PM-4	PM-4 (a) (2)	CCI-000170	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.	DoDI 8510.01 and the Knowledge Service meet the DoD requirements to maintain a process to document the remedial information security actions that mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation. DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8510.01 and the Knowledge Service.	DoDI 8510.01 and the Knowledge Service meet the DoD requirements to maintain a process to document the remedial information security actions that mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation. DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8510.01 and the Knowledge Service.
PM-4	PM-4 (a) (3)	CCI-002992	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.	DoDI 8510.01 and the Knowledge Service meet the DoD requirements to implement a process ensuring that the plans of action and milestones for the security program are reported in accordance with OMB FISMA reporting requirements. DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8510.01 and the Knowledge Service.	DoDI 8510.01 and the Knowledge Service meet the DoD requirements to implement a process ensuring that the plans of action and milestones for the security program are reported in accordance with OMB FISMA reporting requirements. DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8510.01 and the Knowledge Service.
PM-4	PM-4 (b)	CCI-002993	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.	The organization being inspected/assessed documents and implements a process to review 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. The organization must maintain a record of reviews.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of reviews to ensure the organization being inspected/assessed 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.
PM-5	PM-5	CCI-000207	The organization develops and maintains an inventory of its information systems.	DITPR is the inventory for all DoD information systems. The organization being inspected/assessed must register and maintain their information systems in DITPR.	DITPR is the inventory for all DoD information systems. The organization conducting the inspection/assessment obtains and examines the inventory of information systems via DITPR to ensure the organization being inspected/assessed registers their information systems in DITPR.
PM-6	PM-6	CCI-000209	The organization develops the results of information security measures of performance.	The Federal Information Systems Management Act (FISMA) meets the DoD requirements for information security performance measures of performance.	The Federal Information Systems Management Act (FISMA) meets the DoD requirements for information security performance measures of performance. DoD organizations are automatically compliant with this control as they are covered at the DoD level by FISMA.
PM-6	PM-6	CCI-000210	The organization monitors the results of information security measures of performance.	The Federal Information Systems Management Act (FISMA) meets the DoD requirements for information security performance measures of performance.	The Federal Information Systems Management Act (FISMA) meets the DoD requirements for information security performance measures of performance. DoD organizations are automatically compliant with this control as they are covered at the DoD level by FISMA.
PM-6	PM-6	CCI-000211	The organization reports on the results of information security measures of performance.	The organization being inspected/assessed reports the results of information security measures of performance IAW FISMA reporting guidance.	The organization conducting the inspection/assessment obtains and examines FISMA reporting documentation.

PM-7	PM-7	CCI-000212	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.	The GIG IA Architecture meets the DoD requirements for enterprise architecture. DoD components are automatically compliant with this CCI as they covered at the DoD level.	The GIG IA Architecture meets the DoD requirements for enterprise architecture. DoD components are automatically compliant with this CCI as they covered at the DoD level.
PM-8	PM-8	CCI-000216	The organization develops and documents a critical infrastructure and key resource protection plan that addresses information security issues.	DoDD 3020.40 meets the DoD requirement for the development of a critical infrastructure and key resource protection plan. DoD components are automatically compliant with this control as they are covered by the DoD level, DoDD 3020.40.	DoDD 3020.40 meets the DoD requirement for the development of a critical infrastructure and key resource protection plan. DoD components are automatically compliant with this control as they are covered by the DoD level, DoDD 3020.40.
PM-8	PM-8	CCI-001640	The organization updates the critical infrastructure and key resources protection plan that addresses information security issues.	DoDD 3020.40 meets the DoD requirement for the development of a critical infrastructure and key resource protection plan. DoD components are automatically compliant with this control as they are covered by the DoD level, DoDD 3020.40.	DoDD 3020.40 meets the DoD requirement for the development of a critical infrastructure and key resource protection plan. DoD components are automatically compliant with this control as they are covered by the DoD level, DoDD 3020.40.
PM-9	PM-9 (a)	CCI-000227	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.	DoD Risk Management Framework meets the requirement for a comprehensive organizational risk strategy. DoD components are automatically compliant with this CCI because they are covered by the DoD Risk Management Framework (DoDI 8510.01).	DoD Risk Management Framework meets the requirement for a comprehensive organizational risk strategy. DoD components are automatically compliant with this CCI because they are covered by DoD Risk Management Framework (DoDI 8510.01).
PM-9	PM-9 (b)	CCI-000228	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.	DoD Risk Management Framework meets the requirement for a comprehensive organizational risk strategy. DoD components are automatically compliant with this CCI because they are covered by the DoD Risk Management Framework (DoDI 8510.01).	DoD Risk Management Framework meets the requirement for a comprehensive organizational risk strategy. DoD components are automatically compliant with this CCI because they are covered by DoD Risk Management Framework (DoDI 8510.01).
PM-9	PM-9 (c)	CCI-002994	The organization reviews and updates the risk management strategy in accordance with organization-defined frequency or as required, to address organizational changes.	DoD Risk Management Framework meets the requirement for a comprehensive organizational risk strategy. DoD components are automatically compliant with this CCI because they are covered by the DoD Risk Management Framework (DoDI 8510.01).	DoD Risk Management Framework meets the requirement for a comprehensive organizational risk strategy. DoD components are automatically compliant with this CCI because they are covered by DoD Risk Management Framework (DoDI 8510.01).
PM-9	PM-9 (c)	CCI-002995	The organization defines the frequency to review and update the risk management strategy to address organizational changes.	DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance
PM-10	PM-10 (a)	CCI-000229	The organization documents the security state of organizational information systems and the environments in which those systems operate through security authorization processes.	DoDI 8510.01 meets the DoD requirement to manage the security authorization process. DoD components are automatically compliant with this CCI because they are covered at the DoD level, DoDI 8510.01.	DoDI 8510.01 meets the DoD requirement to manage the security authorization process. DoD components are automatically compliant with this CCI because they are covered at the DoD level, DoDI 8510.01.
PM-10	PM-10 (a)	CCI-000230	The organization tracks the security state of organizational information systems and the environments in which those systems operate through security authorization processes.	DoDI 8510.01 meets the DoD requirement to manage the security authorization process. DoD components are automatically compliant with this CCI because they are covered at the DoD level, DoDI 8510.01.	DoDI 8510.01 meets the DoD requirement to manage the security authorization process. DoD components are automatically compliant with this CCI because they are covered at the DoD level, DoDI 8510.01.
PM-10	PM-10 (a)	CCI-000231	The organization reports the security state of organizational information systems and the environments in which those systems operate through security authorization processes.	DoDI 8510.01 meets the DoD requirement to manage the security authorization process. DoD components are automatically compliant with this CCI because they are covered at the DoD level, DoDI 8510.01.	DoDI 8510.01 meets the DoD requirement to manage the security authorization process. DoD components are automatically compliant with this CCI because they are covered at the DoD level, DoDI 8510.01.
PM-10	PM-10 (b)	CCI-000233	The organization designates individuals to fulfill specific roles and responsibilities within the organizational risk management process.	DoDI 8510.01 meets the DoD requirement to designate roles and responsibilities for the risk management process. DoD components are automatically compliant with this CCI because they are covered at the DoD level, DoDI 8510.01.	DoDI 8510.01 meets the DoD requirement to designate roles and responsibilities for the risk management process. DoD components are automatically compliant with this CCI because they are covered at the DoD level, DoDI 8510.01.

PM-10	PM-10 (c)	CCI-000234	The organization fully integrates the security authorization processes into an organization-wide risk management program.	DoDI 8510.01 meets the DoD requirement to fully integrate the security authorization process. DoD components are automatically compliant with this CCI because they are covered at the DoD level, DoDI 8510.01.	DoDI 8510.01 meets the DoD requirement to fully integrate the security authorization process. DoD components are automatically compliant with this CCI because they are covered at the DoD level, DoDI 8510.01.
PM-11	PM-11 (a)	CCI-000235	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.	DoDI 8510.01 meets the DoD requirement to define mission/business processes. DoD components are automatically complaint with this control as they are covered at the DoD level, DoDI 8510.01.	DoDI 8510.01 meets the DoD requirement to define mission/business processes. DoD components are automatically complaint with this control as they are covered at the DoD level, DoDI 8510.01.
PM-11	PM-11 (b)	CCI-000236	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.	The organization being inspected/asssessed determines information protection needs IAW CNSSI 1253 and as identified in RA-2.	The organization conducting the inspection/assessment obtains and examines the security plan to ensure the security categorization has been documented IAW CNSSI 1253.
PM-12	PM-12	CCI-002996	The organization implements an insider threat program that includes a cross-discipline insider threat incident handling team.	The organization being inspected/assessed documents and implements an insider threat program that includes a cross-discipline insider threat incident handling team.	The organization conducting the inspection/assessment obtains and examines the documented insider threat program to ensure the organization being inspected/assessed implements an insider threat program that includes a cross-discipline insider threat incident handling team.
PM-13	PM-13	CCI-002997	The organization establishes an information security workforce development and improvement program.	DoD 8570.01-M, "Information Assurance Workforce Improvement Program" meets the DoD requirement to establish an information security workforce development and improvement program. DoD components are automatically complaint with this control as they are covered at the DoD level, DoDI 8570.01-M.	DoD 8570.01-M meets the DoD requirement to establish an information security workforce development and improvement program. DoD components are automatically complaint with this control as they are covered at the DoD level, DoDI 8570.01-M.
PM-14	PM-14 (a) (1)	CCI-002998	The organization implements a process for ensuring that organizational plans for conducting security testing activities associated with organizational information systems are developed.	The organization being inspected/assessed documents and implements a process for ensuring that organizational plans for conducting security testing activities associated with organizational information systems are developed.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed implements a process for ensuring that organizational plans for conducting security testing activities associated with organizational information systems are developed.
PM-14	PM-14 (a) (1)	CCI-002999	The organization implements a process for ensuring that organizational plans for conducting security testing activities associated with organizational information systems are maintained.	The organization being inspected/assessed documents and implements a process for ensuring that organizational plans for conducting security testing activities associated with organizational information systems are maintained.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed implements a process for ensuring that organizational plans for conducting security testing activities associated with organizational information systems are maintained.
PM-14	PM-14 (a) (1)	CCI-003000	The organization implements a process for ensuring that organizational plans for conducting security training activities associated with organizational information systems are developed.	The organization being inspected/assessed documents and implements a process for ensuring that organizational plans for conducting security training activities associated with organizational information systems are developed.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed implements a process for ensuring that organizational plans for conducting security training activities associated with organizational information systems are developed.
PM-14	PM-14 (a) (1)	CCI-003001	The organization implements a process for ensuring that organizational plans for conducting security training activities associated with organizational information systems are maintained.	The organization being inspected/assessed documents and implements a process for ensuring that organizational plans for conducting security training activities associated with organizational information systems are maintained.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed implements a process for ensuring that organizational plans for conducting security training activities associated with organizational information systems are maintained.
PM-14	PM-14 (a) (1)	CCI-003002	The organization implements a process for ensuring that organizational plans for conducting security monitoring activities associated with organizational information systems are developed.	The organization being inspected/assessed documents and implements a process for ensuring that organizational plans for conducting security monitoring activities associated with organizational information systems are developed.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed implements a process for ensuring that organizational plans for conducting security monitoring activities associated with organizational information systems are developed.
PM-14	PM-14 (a) (1)	CCI-003003	The organization implements a process for ensuring that organizational plans for conducting security monitoring activities associated with organizational information systems are maintained.	The organization being inspected/assessed documents and implements a process for conducting security monitoring activities associated with organizational information systems are maintained.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed implements a process for ensuring that organizational plans for conducting security monitoring activities associated with organizational information systems are maintained.

PM-14	PM-14 (a) (2)	CCI-003004	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.	The organization being inspected/assessed documents and 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. The organization must maintain records of execution.	The organization conducting the inspection/assessment obtains and examines the documented process as well as records of execution to ensure the organization being inspected/assessed 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.
PM-14	PM-14 (a) (2)	CCI-003005	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.	The organization being inspected/assessed documents and 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. The organization must maintain records of execution.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the records of execution to ensure the organization being inspected/assessed 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.
PM-14	PM-14 (a) (2)	CCI-003006	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.	The organization being inspected/assessed documents and 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. The organization must maintain records of execution.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the records of execution to ensure the organization being inspected/assessed 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.
PM-14	PM-14 (b)	CCI-003007	The organization reviews testing plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.	The organization being inspected/assessed documents and implements a process to review testing plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions. The organization must maintain a record of reviews.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of reviews to ensure the organization being inspected/assessed reviews testing plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.
PM-14	PM-14 (b)	CCI-003008	The organization reviews training plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.	The organization being inspected/assessed reviews training plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions. The organization must maintain a record of reviews.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of reviews to ensure the organization being inspected/assessed reviews training plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.
PM-14	PM-14 (b)	CCI-003009	The organization reviews monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.	The organization being inspected/assessed reviews monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions. The organization must maintain a record of reviews.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of reviews to ensure the organization being inspected/assessed reviews monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.
PM-15	PM-15 (a)	CCI-003010	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.	The organization being inspected/assessed establishes and institutionalizes contact with selected groups and associations within the security community to facilitate ongoing security education and training for organizational personnel.	The organization conducting the inspection/assessment obtains and examines artifacts showing contact to ensure the organization being inspected/assessed establishes and institutionalizes contact with selected groups and associations within the security community to facilitate ongoing security education and training for organizational personnel.
PM-15	PM-15 (b)	CCI-003011	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.	The organization being inspected/assessed establishes and institutionalizes contact with selected groups and associations within the security community to maintain currency with recommended security practices, techniques, and technologies.	The organization conducting the inspection/assessment obtains and examines artifacts showing contact to ensure the organization being inspected/assessed establishes and institutionalizes contact with selected groups and associations within the security community to maintain currency with recommended security practices, techniques, and technologies.
PM-15	PM-15 (c)	CCI-003012	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.	The organization being inspected/assessed establishes and institutionalizes contact with selected groups and associations within the security community to share current security-related information including threats, vulnerabilities, and incidents.	The organization conducting the inspection/assessment obtains and examines artifacts showing contact to ensure the organization being inspected/assessed establishes and institutionalizes contact with selected groups and associations within the security community to share current security-related information including threats, vulnerabilities, and incidents.
PM-16	PM-16	CCI-003013	The organization implements a threat awareness program that includes a cross-organization information-sharing capability.	The organization being inspected/assessed documents and implements a threat awareness program that includes a cross-organization information-sharing capability.	The organization conducting the inspection/assessment obtains and examines the documented threat awareness program to ensure the organization being inspected/assessed implements a threat awareness program that includes a cross-organization information-sharing capability.

PS-1	PS-1 (a)	CCI-003017	The organization defines the personnel or roles to whom a personnel security policy is disseminated.	DoD has defined the roles as organizational personnel with access control responsibilities.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the roles as organizational personnel with access control responsibilities.
PS-1	PS-1 (a)	CCI-003018	The organization defines the personnel or roles to whom the personnel security procedures are disseminated.	DoD has defined the roles as organizational personnel with access control responsibilities.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the roles as organizational personnel with access control responsibilities.
PS-1	PS-1 (a) (1)	CCI-001504	The organization develops and documents a personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	DoD 5200.2-R meets the DoD requirements for personnel security policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoD 5200.2-R.	DoD 5200.2-R meets the DoD requirements for personnel security policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoD 5200.2-R.
PS-1	PS-1 (a) (1)	CCI-001505	The organization disseminates a personnel security policy to organization-defined personnel or roles.	DoD disseminates DoD 5200.2-R via the DoD Issuance site: http://www.dtic.mil/whs/directives/corres/pub1.html to meet the DoD requirements for personnel security policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoD 5200.2-R.	DoD 5200.2-R meets the DoD requirements for personnel security policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoD 5200.2-R.
PS-1	PS-1 (a) (2)	CCI-001509	The organization develops and documents procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.	DoD 5200.2-R meets the DoD requirements for personnel security policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoD 5200.2-R.	DoD 5200.2-R meets the DoD requirements for personnel security policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoD 5200.2-R.
PS-1	PS-1 (a) (2)	CCI-001510	The organization disseminates personnel security procedures to organization-defined personnel or roles.	DoD disseminates DoD 5200.2-R via the DoD Issuance site: http://www.dtic.mil/whs/directives/corres/pub1.html to meet the DoD requirements for personnel security policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoD 5200.2-R.	DoD 5200.2-R meets the DoD requirements for personnel security policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoD 5200.2-R.
PS-1	PS-1 (b) (1)	CCI-001507	The organization defines the frequency to review and update the current personnel security policy.	DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.
PS-1	PS-1 (b) (1)	CCI-001506	The organization reviews and updates the current personnel security policy in accordance with organization-defined frequency.	DoD 5200.2-R meets the DoD requirements for personnel security policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoD 5200.2-R.	DoD 5200.2-R meets the DoD requirements for personnel security policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoD 5200.2-R.
PS-1	PS-1 (b) (2)	CCI-001508	The organization defines the frequency to review and update the current personnel security procedures.	DoD has defined the frequency as reviewed annually - updated as appropriate.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as reviewed annually - updated as appropriate.
PS-1	PS-1 (b) (2)	CCI-001511	The organization reviews and updates the current personnel security procedures in accordance with organization-defined frequency.	DoD 5200.2-R meets the DoD requirements for personnel security policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoD 5200.2-R.	DoD 5200.2-R meets the DoD requirements for personnel security policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoD 5200.2-R.
PS-2	PS-2 (a)	CCI-001512	The organization assigns a risk designation to all organizational positions.	The organization being inspected/assessed will designate and document all organizational positions, to include government and contract positions, with the appropriate ADP/IT level designation, IAW DoD 5200.2-R.	The organization conducting the inspection/assessment obtains and examines documentation of the ADP/IT level designations.
PS-2	PS-2 (b)	CCI-001513	The organization establishes screening criteria for individuals filling organizational positions.	DoD 5200.2-R meets the DoD requirements for establishing screening criteria for individuals filling organizational positions. DoD organizations are automatically compliant with this control as they are covered at the DoD level by DoD 5200.2-R.	DoD 5200.2-R meets the DoD requirements for establishing screening criteria for individuals filling organizational positions. DoD organizations are automatically compliant with this control as they are covered at the DoD level by DoD 5200.2-R.

PS-2	PS-2 (c)	CCI-001514	The organization reviews and updates position risk designations in accordance with organization-defined frequency.	The organization being inspected/assessed reviews position risk designations annually and revises designations as required based on the reviews. Records of these reviews must be maintained as an audit trail. DoD has defined the frequency as annually.	The organization conducting the inspection/assessment reviews the audit records of the position designation reviews to ensure reviews are done annually. DoD has defined the frequency as annually.
PS-2	PS-2 (c)	CCI-001515	The organization defines the frequency to review and update position risk designations.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.
PS-3	PS-3 (a)	CCI-001516	The organization screens individuals prior to authorizing access to the information system.	The organization being inspected/assessed will screen all government and contract personnel to ensure they meet the appropriate ADP/IT level designation requirements IAW DoD 5200.2-R prior to authorizing access to the information system.	The organization conducting the inspection/assessment obtains and examines the information system access list (AC-2) and compares a sampling of authorized users to manning documents (PS-2) to ensure access was granted appropriately IAW ADP/IT level designation requirements within DoD 5200.2-R.
PS-3	PS-3 (b)	CCI-001517	The organization rescreens individuals with authorized access to the information system according to organization-defined conditions requiring rescreening, and where rescreening is so indicated, the organization-defined frequency of such rescreening.	The information system owner will rescreen individuals according to system owner defined list of conditions requiring rescreening (CCI-001518) individuals for access to the information system and frequency (CCI - 001519) of such rescreening. Rescreening actions will be maintained as an audit trail (AU-2).	The organization conducting the inspection/assessment obtains and examines audit records of rescreening actions to ensure the system owner is rescreening individuals according to a system owner-defined list of conditions requiring rescreening and, where re-screening is so indicated, based on the system owner-defined frequency of such rescreening.
PS-3	PS-3 (b)	CCI-001518	The organization defines the conditions requiring rescreening of individuals with authorized access to the information system.	The information system owner will develop and document the list of conditions requiring rescreening individuals for access to the information system. DoD has determined the list of conditions is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documentation of conditions requiring rescreening of individuals for access to the information system. DoD has determined the list of conditions is not appropriate to define at the Enterprise level.
PS-3	PS-3 (b)	CCI-001519	The organization defines the frequency for rescreening individuals with authorized access to the information system when organization-defined conditions requiring rescreening are met.	The information system owner will define and document the required frequency of rescreening for access to the information system. DoD has determined the frequency is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documentation defining the required frequency for rescreening individuals for access to the system. DoD has determined the frequency is not appropriate to define at the Enterprise level.
PS-4	PS-4 (a)	CCI-003022	The organization defines the time period to disable information system access upon termination of individual employment.	DoD has defined the time period as immediately.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as immediately.
PS-4	PS-4 (a)	CCI-001522	The organization, upon termination of individual employment, disables information system access within organization-defined time period.	The organization being inspected/assessed upon termination of individual employment, terminates information system access immediately and IAW organization security policy and procedures. The organization must retain an audit trail of account termination actions (AU-2). DoD has defined the time period as immediately.	The organization conducting the inspection/assessment obtains and examines organizational security policy and procedures documentation and audit records of account termination actions to ensure account termination actions are conducted immediately and IAW organizational security policy and procedures. DoD has defined the time period as immediately.
PS-4	PS-4 (b)	CCI-003023	The organization, upon termination of individual employment, terminates/revokes any authenticators/credentials associated with the individual.	The organization being inspected/assessed documents and implements a process to terminate/revoke any authenticators/credentials associated with the individual upon termination of individual employment. The organization must maintain records of termination/revocation of any authenticators/credentials.	The organization conducting the inspection/assessment obtains and examines the documented process as well as a sampling of records of termination/revocation of any authenticators/credentials to ensure the organization being inspected/assessed terminates/revokes any authenticators/credentials associated with the individual upon termination of individual employment.
PS-4	PS-4 (c)	CCI-003024	The organization defines information security topics to be discussed while conducting exit interviews.	The organization being inspected/assessed defines and documents information security topics to be discussed while conducting exit interviews. DoD has determined the information security topics are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented information security topics to ensure the organization being inspected/assessed defines information security topics to be discussed while conducting exit interviews. DoD has determined the information security topics are not appropriate to define at the Enterprise level.

PS-4	PS-4 (c)	CCI-001523	The organization, upon termination of individual employment, conducts exit interviews that include a discussion of organization-defined information security topics.	The organization being inspected/assessed, conducts exit interviews that include a discussion of information security topics defined in PS-4, CCI 3024 upon termination of individual employment IAW organization security policy and procedures. The organization must retain an audit trail of conducted exit interviews (AU-2)	The organization conducting the inspection/assessment obtains and examines documentation of departed personnel and the audit trail of conducted exit interviews to ensure all departed personnel had exit interviews conducted that include a discussion of information security topics defined in PS-4, CCI 3024.
PS-4	PS-4 (d)	CCI-001524	The organization, upon termination of individual employment, retrieves all security-related organizational information systems-related property.	The organization being inspected/assessed upon termination of individual employment retrieves all security-related organizational information systems-related property IAW organization security policy and procedures. The organization must retain an audit trail of all retrieved security-related organizational information systems-related property (AU-2).	The organization conducting the inspection/assessment obtains and examines appropriate organization security-related organizational information systems-related property documentation/logs and compares to audit trail of all retrieved security-related organizational information systems-related property (AU-2) to ensure all property has been retrieved.
PS-4	PS-4 (e)	CCI-001525	The organization, upon termination of individual employment, retains access to organizational information formerly controlled by terminated individual.	The organization being inspected/assessed upon termination of individual employment retains access to organizational information formerly controlled by terminated individual IAW organization security policy and procedures. Organizational information formerly controlled by terminated individuals generally refers to online work-product including email files.	The organization conducting the inspection/assessment interviews appropriate IT and security personnel to validate the organization has procedures in place which, upon termination of individual's employment, will ensure it retains access to organizational information formerly controlled by the terminated individual.
PS-4	PS-4 (e)	CCI-001526	The organization, upon termination of individual employment, retains access to organizational information systems formerly controlled by terminated individual.	The organization being inspected/assessed upon termination of individual employment retains access to organizational information systems formerly controlled by terminated individual IAW organization security policy and procedures. Organizational information systems formerly controlled by terminated individuals generally refers to issued hardware (e.g. laptops, BlackBerrys, PEDs, removable media, etc.)	The organization conducting the inspection/assessment interviews appropriate IT and security personnel to validate the organization has procedures in place which, upon termination of individual's employment, will ensure it retains access to organizational information systems formerly controlled by the terminated individual.
PS-4	PS-4 (f)	CCI-003025	The organization defines personnel or roles to notify upon termination of individual employment.	DoD has defined the personnel or roles as at a minimum, the ISSO and personnel responsible for revoking credentials.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as at a minimum, the ISSO and personnel responsible for revoking credentials.
PS-4	PS-4 (f)	CCI-003026	The organization defines the time period in which to notify organization-defined personnel or roles upon termination of individual employment.	DoD has defined the time period as immediately or within 24 hours.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as immediately or within 24 hours.
PS-4	PS-4 (f)	CCI-003016	The organization, upon termination of individual employment, notifies organization-defined personnel or roles within an organization-defined time period.	The organization being inspected/assessed notifies at a minimum, the ISSO and personnel responsible for revoking credentials immediately or within 24 hours upon termination of individual employment. The organization must maintain records of termination notification. DoD has defined the personnel or roles as at a minimum, the ISSO and personnel responsible for revoking credentials. DoD has defined the time period as immediately or within 24 hours.	The organization conducting the inspection/assessment obtains and examines records of termination notification to ensure the organization being inspected/assessed notifies at a minimum, the ISSO and personnel responsible for revoking credentials immediately or within 24 hours upon termination of individual employment. DoD has defined the personnel or roles as at a minimum, the ISSO and personnel responsible for revoking credentials. DoD has defined the time period as immediately or within 24 hours.
PS-4 (1)	PS-4 (1) (a)	CCI-003027	The organization notifies terminated individuals of applicable, legally binding post-employment requirements for the protection of organizational information.	The organization being inspected/assessed notifies terminated individuals of applicable, legally binding post-employment requirements for the protection of organizational information. The organization must maintain a record of notifications of post-employment requirements.	The organization conducting the inspection/assessment obtains and examines the record of notifications of post-employment requirements to ensure the organization being inspected/assessed notifies terminated individuals of applicable, legally binding post-employment requirements for the protection of organizational information.
PS-4 (1)	PS-4 (1) (b)	CCI-003028	The organization requires terminated individuals to sign an acknowledgment of post-employment requirements as part of the organizational termination process.	The organization being inspected/assessed documents within their personnel security procedures the requirement for terminated individuals to sign an acknowledgment of post-employment requirements as part of the organizational termination process.	The organization conducting the inspection/assessment obtains and examines the personnel security procedures and a sampling of signed acknowledgments of post-employment requirements to ensure the organization being inspected/assessed requires terminated individuals to sign an acknowledgment of post-employment requirements as part of the organizational termination process.

PS-5	PS-5 (a)	CCI-001527	The organization reviews and confirms 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.	The organization being inspected/assessed reviews and confirms ongoing operational need for logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization. The organization must maintain an audit trail of reviews.	The organization conducting the inspection/assessment obtains and examines the audit trail of reviews to ensure that the organization has confirmed the ongoing operational need for logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization.
PS-5	PS-5 (b)	CCI-001528	The organization initiates organization-defined transfer or reassignment actions within an organization-defined time period following the formal personnel transfer action.	The organization being inspected/assessed initiates transfer or reassignment actions to ensure all system accesses no longer required are removed and actions to ensure all system accesses required due to the individual's new position are granted immediately when personnel are reassigned or transferred to other positions. DoD defines transfer or reassignment actions as actions to ensure all system accesses no longer required are removed. DoD defines the time period as immediately.	The organization conducting the inspection/assessment obtains and examines appropriate organization security-related organizational physical and logical access documentation/logs and compares to transferred personnel documentation to ensure appropriate logical and physical access have been revoked for previous positions and granted for new positions immediately. DoD defines the time period as immediately.
PS-5	PS-5 (b)	CCI-001529	The organization defines transfer or reassignment actions to initiate within an organization-defined time period following the formal personnel transfer action.	DoD defines transfer or reassignment actions as actions to ensure all system accesses no longer required are removed.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD defines transfer or reassignment actions as actions to ensure all system accesses no longer required are removed.
PS-5	PS-5 (b)	CCI-001530	The organization defines the time period within which the organization initiates organization-defined transfer or reassignment actions, following the formal personnel transfer action.	DoD defines the time period as immediately.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD defines the time period as immediately.
PS-5	PS-5 (c)	CCI-003031	The organization modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer.	The organization being inspected/assessed documents and implements a process to modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer.	The organization conducting the inspection/assessment obtains and examines the documented process and a sampling of accounts of users recently transferred or reassigned to ensure the organization being inspected/assessed modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer.
PS-5	PS-5 (d)	CCI-003032	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.	The organization being inspected/assessed notifies at a minimum, the ISSO and personnel responsible for transferring credentials within 24 hours when individuals are transferred or reassigned to other positions within the organization. The organization must maintain records of transfer/reassignment notifications. DoD has defined the personnel or roles as at a minimum, the ISSO and personnel responsible for transferring credentials. DoD has defined the time period as within 24 hours.	The organization conducting the inspection/assessment obtains and examines records of transfer/reassignment notifications to ensure the organization being inspected/assessed notifies at a minimum, the ISSO and personnel responsible for transferring credentials within 24 hours when individuals are transferred or reassigned to other positions within the organization. DoD has defined the personnel or roles as at a minimum, the ISSO and personnel responsible for transferring credentials. DoD has defined the time period as within 24 hours.
PS-5	PS-5 (d)	CCI-003033	The organization defines personnel or roles to be notified when individuals are transferred or reassigned to other positions within the organization.	DoD has defined the personnel or roles as at a minimum, the ISSO and personnel responsible for transferring credentials.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as at a minimum, the ISSO and personnel responsible for transferring credentials.
PS-5	PS-5 (d)	CCI-003034	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.	DoD has defined the time period as immediately.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as immediately.
PS-6	PS-6 (a)	CCI-003035	The organization develops and documents access agreements for organizational information systems.	The organization being inspected/assessed develops and documents access agreements for organizational information systems.	The organization conducting the inspection/assessment obtains and examines the documented access agreements to ensure the organization being inspected/assessed develops and documents access agreements for organizational information systems.
PS-6	PS-6 (b)	CCI-001533	The organization defines the frequency to review and update the access agreements.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.

PS-6	PS-6 (b)	CCI-001532	The organization reviews and updates the access agreements in accordance with organization-defined frequency.	The organization being inspected/assessed reviews/updates the access agreements annually of employees who have signed access agreements. The purpose of this review/update is to ensure access agreements are current and departed employees no longer have access agreements. The organization must maintain an audit trail of the review and update activity for review. DoD has defined the frequency as annually.	The organization conducting the inspection/assessment obtains and examines the audit trail to ensure review/update occurred annually and departed employees no longer have valid access agreements.
PS-6	PS-6 (c) (1)	CCI-001531	The organization ensures that individuals requiring access to organizational information and information systems sign appropriate access agreements prior to being granted access.	The organization being inspected/assessed will ensure all individuals have appropriate access agreements in place prior to being granted access to information and information systems. DD Form 2875 is the accepted DoD methodology of requesting and granting of access to information and information systems.	The organization conducting the inspection/assessment obtains a list of organizational individuals with active accounts and validates the existence of signed DD Form 2875 (paper or electronic) associated with a sampling of individuals selected from the list.
PS-6	PS-6 (c) (2)	CCI-003037	The organization defines the frequency for individuals requiring access to organization information and information systems to re-sign access agreements.	DoD has defined the frequency as when there is a change to the user's level of access.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as when there is a change to the user's level of access.
PS-6	PS-6 (c) (2)	CCI-003036	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.	The organization being inspected/assessed requires that individuals re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or when there is a change to the user's level of access. DoD has defined the frequency as when there is a change to the user's level of access.	The organization conducting the inspection/assessment obtains and examines a sampling of re-signed access agreements to ensure the organization being inspected/assessed requires that individuals re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or when there is a change to the user's level of access. DoD has defined the frequency as when there is a change to the user's level of access.
PS-6 (3)	PS-6 (3) (a)	CCI-003038	The organization notifies individuals of applicable, legally binding post-employment requirements for protection of organizational information.	The organization being inspected/assessed notifies individuals of applicable, legally binding post-employment requirements for protection of organizational information. The organization must maintain records of notifications of post-employment requirements for protection of organizational information.	The organization conducting the inspection/assessment obtains and examines the records of notifications of post-employment requirements for protection of organizational information to ensure the organization being inspected/assessed notifies individuals of applicable, legally binding post-employment requirements for protection of organizational information.
PS-6 (3)	PS-6 (3) (b)	CCI-003039	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.	The organization being inspected/assessed documents and implements a process to require 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.	The organization conducting the inspection/assessment obtains and examines the documented process and a sampling of signed acknowledgements to ensure the organization being inspected/assessed 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.
PS-7	PS-7 (a)	CCI-001539	The organization establishes personnel security requirements including security roles and responsibilities for third-party providers.	DoD 5220.22-M, DoD 5220.22-R, DoD 5200.2-R, DoD 8570.01-M and DoDI 3020.41 meet the DoD personnel security requirements including security roles and responsibilities for third-party providers. DoD Components are automatically compliant with this control because they are covered by the DoD level policies, DoD 5220.22-M, DoD 5220.22-R, DoD 5200.2-R, DoD 8570.01-M and DoDI 3020.41.	DoD 5220.22-M, DoD 5220.22-R, DoD 5200.2-R, DoD 8570.01-M and DoDI 3020.41 meet the DoD personnel security requirements including security roles and responsibilities for third-party providers. DoD Components are automatically compliant with this control because they are covered by the DoD level policies, DoD 5220.22-M, DoD 5220.22-R, DoD 5200.2-R, DoD 8570.01-M and DoDI 3020.41.
PS-7	PS-7 (b)	CCI-003040	The organization requires third-party providers to comply with personnel security policies and procedures established by the organization.	The organization being inspected/assessed documents and implements a process to require third-party providers to comply with personnel security policies and procedures established by the organization.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed requires third-party providers to comply with personnel security policies and procedures established by the organization.
PS-7	PS-7 (c)	CCI-001540	The organization documents personnel security requirements for third-party providers.	The organization being inspected/assessed documents personnel security requirements for third-party providers.	The organization conducting the inspection/assessment obtains and examines the personnel security requirements to ensure the organization being inspected/assessed documents personnel security requirements for third-party providers.

PS-7	PS-7 (d)	CCI-003042	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.	DoD has defined the personnel or roles as at a minimum, the ISSO and personnel responsible for transferring credentials.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as at a minimum, the ISSO and personnel responsible for transferring credentials.
PS-7	PS-7 (d)	CCI-003043	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.	DoD has defined the time period as immediately.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as immediately.
PS-7	PS-7 (d)	CCI-003041	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.	The organization being inspected/assessed documents and implements a process to require third-party providers to notify at a minimum, the ISSO and personnel responsible for transferring credentials of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges immediately. DoD has defined the personnel or roles as at a minimum, the ISSO and personnel responsible for transferring credentials. DoD has defined the time period as immediately.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed requires third-party providers to notify at a minimum, the ISSO and personnel responsible for transferring credentials of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges immediately. DoD has defined the personnel or roles as at a minimum, the ISSO and personnel responsible for transferring credentials. DoD has defined the time period as immediately.
PS-7	PS-7 (e)	CCI-001541	The organization monitors third-party provider compliance with personnel security requirements.	The organization being inspected/assessed monitors third-party provider compliance with personnel security requirements. The organization must maintain an audit trail of monitoring activity.	The organization conducting the inspection/assessment obtains and examines the audit trail of monitoring activity to ensure the organization being inspected/assessed monitors third-party provider compliance with personnel security requirements.
PS-8	PS-8 (a)	CCI-001542	The organization employs a formal sanctions process for individuals failing to comply with established information security policies and procedures.	The organization being inspected/assessed will develop formal procedures within the organizational security policy to employ formal sanctions for personnel failing to comply with established information security policies and procedures.	The organization conducting the inspection/assessment obtains and examines the organizational security policy to ensure it addresses formal procedures for sanctions and interviews security personnel to validate the organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.
PS-8	PS-8 (b)	CCI-003046	The organization defines the time period to notify organization-defined personnel or roles when a formal employee sanctions process is initiated.	DoD has defined the time period as immediately.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as immediately.
PS-8	PS-8 (b)	CCI-003044	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.	The organization being inspected/assessed notifies at a minimum, the ISSO immediately when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction. The organization must maintain records of notifications of employee sanctions. DoD has defined the personnel or roles as at a minimum, the ISSO. DoD has defined the time period as immediately.	The organization conducting the inspection/assessment obtains and examines the records of notifications of employee sanctions to ensure the organization being inspected/assessed notifies at a minimum, the ISSO immediately when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction. DoD has defined the personnel or roles as at a minimum, the ISSO. DoD has defined the time period as immediately.
PS-8	PS-8 (b)	CCI-003045	The organization defines personnel or roles whom are to be notified when a formal employee sanctions process is initiated.	DoD has defined the personnel or roles as at a minimum, the ISSO.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as at a minimum, the ISSO.
RA-1	RA-1 (a)	CCI-002368	The organization defines the personnel or roles to whom the risk assessment policy is disseminated.	DoD has defined the roles as at a minimum, the ISSM and ISSO.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as at a minimum, the ISSM and ISSO.
RA-1	RA-1 (a)	CCI-002369	The organization defines the personnel or roles to whom the risk assessment procedures are disseminated.	DoD has defined the roles as at a minimum, the ISSM and ISSO.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as at a minimum, the ISSM and ISSO.

RA-1	RA-1 (a) (1)	CCI-001037	The organization develops and documents a risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	NIST SP 800-30 meets the DoD requirements for risk assessment policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoDi 8510.01 which adopts NIST SP 800-30 as the DoD risk assessment policy.	NIST SP 800-30 meets the DoD requirements for risk assessment policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoDi 8510.01 which adopts NIST SP 800-30 as the DoD risk assessment policy.
RA-1	RA-1 (a) (1)	CCI-001038	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.	NIST SP 800-30 meets the DoD requirements for risk assessment policy and procedures and is disseminated via the NIST publications site: http://csrc.nist.gov/publications/PubsSPs.html DoD Components are automatically compliant with this CCI because they are covered by the DoDi 8510.01 which adopts NIST SP 800-30 as the DoD risk assessment policy.	NIST SP 800-30 meets the DoD requirements for risk assessment policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoDi 8510.01 which adopts NIST SP 800-30 as the DoD risk assessment policy.
RA-1	RA-1 (a) (2)	CCI-001041	The organization develops and documents procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.	NIST SP 800-30 meets the DoD requirements for risk assessment policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoDi 8510.01 which adopts NIST SP 800-30 as the DoD risk assessment policy.	NIST SP 800-30 meets the DoD requirements for risk assessment policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoDi 8510.01 which adopts NIST SP 800-30 as the DoD risk assessment policy.
RA-1	RA-1 (a) (2)	CCI-001042	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.	NIST SP 800-30 meets the DoD requirements for risk assessment policy and procedures and is disseminated via the NIST publications site: http://csrc.nist.gov/publications/PubsSPs.html DoD Components are automatically compliant with this CCI because they are covered by the DoDi 8510.01 which adopts NIST SP 800-30 as the DoD risk assessment policy.	NIST SP 800-30 meets the DoD requirements for risk assessment policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoDi 8510.01 which adopts NIST SP 800-30 as the DoD risk assessment policy.
RA-1	RA-1 (b) (1)	CCI-001039	The organization reviews and updates the current risk assessment policy in accordance with organization-defined frequency.	NIST SP 800-30 meets the DoD requirements for risk assessment policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoDi 8510.01 which adopts NIST SP 800-30 as the DoD risk assessment policy.	NIST SP 800-30 meets the DoD requirements for risk assessment policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoDi 8510.01 which adopts NIST SP 800-30 as the DoD risk assessment policy.
RA-1	RA-1 (b) (1)	CCI-001040	The organization defines the frequency to review and update the current risk assessment policy.	DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.
RA-1	RA-1 (b) (2)	CCI-001043	The organization reviews and updates the current risk assessment procedures in accordance with organization-defined frequency.	NIST SP 800-30 meets the DoD requirements for risk assessment policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoDi 8510.01 which adopts NIST SP 800-30 as the DoD risk assessment policy.	NIST SP 800-30 meets the DoD requirements for risk assessment policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoDi 8510.01 which adopts NIST SP 800-30 as the DoD risk assessment policy.
RA-1	RA-1 (b) (2)	CCI-001044	The organization defines the frequency to review and update the current risk assessment procedures.	DoD has defined the frequency as annually - updated as appropriate.	DoD Components are automatically compliant with this CCI because they are covered by the DoDi 8510.01 which adopts NIST SP 800-30 as the DoD risk assessment policy. DoD has defined the frequency as annually - updated as appropriate.
RA-2	RA-2 (a)	CCI-001045	The organization categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.	The organization being inspected/assessed documents and implements a process to categorize information and the information system in accordance with CNSSI 1253 and applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed categorizes information and the information system in accordance with CNSSI 1253 and applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.
RA-2	RA-2 (b)	CCI-001046	The organization documents the security categorization results (including supporting rationale) in the security plan for the information system.	The organization being inspected/assessed documents the security categorization results (including supporting rationale) in the security plan for the information system IAW CNSSI 1253.	The organization conducting the inspection/assessment obtains and examines the documented security categorization results to ensure the organization being inspected/assessed documents the security categorization results (including supporting rationale) in the security plan for the information system IAW CNSSI 1253.

RA-2	RA-2 (c)	CCI-001047	The organization ensures the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.	The organization being inspected/assessed documents and implements a process IAW CNSSI 1253 to ensure the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed ensures the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.
RA-3	RA-3 (a)	CCI-001048	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.	The organization being inspected/assessed 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. The organization must maintain an audit trail of assessments.	The organization conducting the inspection/assessment obtains and examines the audit trail of assessments to ensure the organization being inspected/assessed 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.
RA-3	RA-3 (b)	CCI-001642	The organization defines the organizational document in which risk assessment results are documented (e.g., security plan, risk assessment report).	DoD has defined the document as a risk assessment report.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the document as a risk assessment report.
RA-3	RA-3 (b)	CCI-001049	The organization documents risk assessment results in the organization-defined document.	The organization being inspected/assessed documents risk assessment results in the risk assessment report. DoD has defined the document as a risk assessment report.	The organization conducting the inspection/assessment obtains and examines the risk assessment report to ensure the organization being inspected/assessed documents risk assessment results in the risk assessment report. DoD has defined the document as a risk assessment report.
RA-3	RA-3 (c)	CCI-001050	The organization reviews risk assessment results on an organization-defined frequency.	The organization being inspected/assessed reviews risk assessment results upon re-accreditation. The organization must maintain a record of reviews. DoD has defined the frequency as upon re-accreditation.	The organization conducting the inspection/assessment obtains and examines the record of reviews to ensure the organization being inspected/assessed reviews risk assessment results upon re-accreditation. DoD has defined the frequency as upon re-accreditation.
RA-3	RA-3 (c)	CCI-001051	The organization defines a frequency for reviewing risk assessment results.	DoD has defined the frequency as upon re-accreditation.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as upon re-accreditation.
RA-3	RA-3 (d)	CCI-002371	The organization defines the personnel or roles whom the risk assessment results will be disseminated.	DoD has defined the personnel or roles as the ISSM, ISSO, AO, and PM.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as the ISSM, ISSO, AO, and PM.
RA-3	RA-3 (d)	CCI-002370	The organization disseminates risk assessment results to organization-defined personnel or roles.	The organization being inspected/assessed documents and implements a process to disseminates risk assessment results to the ISSM, ISSO, AO, and PM. DoD has defined the personnel or roles as the ISSM, ISSO, AO, and PM.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed disseminates the risk assessment results to the ISSM, ISSO, AO, and PM. DoD has defined the personnel or roles as the ISSM, ISSO, AO, and PM.
RA-3	RA-3 (e)	CCI-001052	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.	The organization being inspected/asssessed updates the risk assessment upon re-accreditation 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. DoD has defined the frequency as upon re-accreditation.	The organization conducting the inspection/assessment obtains and examines historical versions of the risk assessment as well as records of changes to the system to ensure the organization being inspected/assessed updates the risk assessment upon re-accreditation 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. DoD has defined the frequency as upon re-accreditation.
RA-3	RA-3 (e)	CCI-001053	The organization defines a frequency for updating the risk assessment.	DoD has defined the frequency as upon re-accreditation.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as upon re-accreditation.
RA-5	RA-5 (a)	CCI-001055	The organization defines a frequency for scanning for vulnerabilities in the information system and hosted applications.	DoD has defined the frequency as every 30 days or as directed by an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs).	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every 30 days or as directed by an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs).

RA-5	RA-5 (a)	CCI-001054	The organization scans for vulnerabilities in the information system and hosted applications on an organization-defined frequency.	The organization being inspected/assessed will define, document, and implement procedures for vulnerability scans of the information system and hosted applications; and scan for vulnerabilities in the information system and hosted applications every 30 days or as directed by an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs). This control is not targeted at security control compliance scanning. DoD has defined the frequency as every 30 days or as directed by an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs).	The organization conducting the inspection/assessment obtains and examines the organization's vulnerability scanning procedures and results for the 90 days preceding the inspection/assessment. If the system in question has not been operational for more than 90 days the organization will provide all available scan(s).
RA-5	RA-5 (a)	CCI-001056	The organization scans for vulnerabilities in the information system and hosted applications when new vulnerabilities potentially affecting the system/applications are identified and reported.	The organization being inspected/assessed will conduct vulnerability scans of the information system and hosted applications when new vulnerabilities potentially affecting the system/applications are identified and reported via authoritative sources (e.g., IAVM, CTO, DTM, STIG, product vendor).	The organization conducting the inspection/assessment obtains and examines the organization's vulnerability scanning procedures and results in order to validate the organization conducts vulnerability scans of its Information System (IS) and hosted applications when new vulnerabilities potentially affecting the IS and/or applications are identified and reported.
RA-5	RA-5 (a)	CCI-001641	The organization defines the process for conducting random vulnerability scans on the information system and hosted applications.	DoD has defined the requirement for vulnerability scanning periodicity of every 30 days. If the organization being inspected/assessed has determined a requirement for random scanning they must document that process. DoD has defined the frequency as every 30 days or as directed by an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs).	The organization conducting the inspection/assessment obtains and examines random vulnerability process documentation (if applicable) to validate the organization has clearly defined and documented a process for conducting random vulnerability scans on the information system and hosted applications. If the organization being inspected/assessed has determined they have no requirement for random scanning, there is no requirement for a process.
RA-5	RA-5 (a)	CCI-001643	The organization scans for vulnerabilities in the information system and hosted applications in accordance with the organization-defined process for random scans.	The organization being inspected/assessed will conduct random vulnerability scans every 30 days or as directed by an authorative source (e.g. IAVM, CTOs, DTMs, STIGs). The organization will document the vulnerability scans as an audit trail for future reference. The audit trail must be maintained IAW DoD, CYBERCOM, or component policies. DoD has defined the frequency as every 30 days or as directed by an authorative source (e.g. IAVM, CTOs, DTMs, STIGs). .	The organization conducting the inspection/assessment obtains and examines the vulnerability scanning results every 30 days or as directed by an authorative source (e.g. IAVM, CTOs, DTMs, STIGs) to verify compliance with the organization being inspected/assessed random vulnerability scanning process. DoD has defined the frequency as every 30 days or as directed by an authorative source (e.g. IAVM, CTOs, DTMs, STIGs).
RA-5	RA-5 (b)	CCI-001057	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.	The organization being inspected/assessed employs the DoD Enterprise scanning tool.	The organization conducting the inspection/assessment obtains and examines the software list or vulnerability scanning procedures to ensure the organization being inspected/assessed employs the DoD Enterprise scanning tool.
RA-5	RA-5 (c)	CCI-001058	The organization analyzes vulnerability scan reports and results from security control assessments.	The organization being inspected/assessed analyzes vulnerability scan reports and security control assessment results with the intent of identifying legitimate vulnerabilities and the relationship between vulnerabilities and security controls.	The organization conducting the inspection/assessment will interview organizational personnel with security control assessment and vulnerability scanning responsibilities. The purpose of the reviews and interviews is to validate the organization is conducting an analysis of the vulnerability scan reports and results from the security control assessments.
RA-5	RA-5 (d)	CCI-001059	The organization remediates legitimate vulnerabilities in organization-defined response times in accordance with an organizational assessment risk.	The organization being inspected/assessed takes corrective actions as appropriate on legitimate vulnerabilities identified in RA-5, CCI 001058 IAW an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs). Audit records of actions must be maintained IAW applicable DoD, CYBERCOM, and/or component policies. DoD has defined the response times as IAW an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs).	The organization conducting the inspection/assessment obtains and examines audit records to validate the organization is taking action to remediate legitimate vulnerabilities within the required response times (IAW an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs). The organization conducting the inspection/assessment may conduct independent vulnerability scans to compare those scan results with audit records of remediation actions. DoD has defined the response times as IAW an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs).

RA-5	RA-5 (d)	CCI-001060	The organization defines response times for remediating legitimate vulnerabilities in accordance with an organization assessment of risk.	DoD has defined the response times as IAW an authoritative source (e.g. IAVM, CTOs, DTMs).	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the response times as IAW an authoritative source (e.g. IAVM, CTOs, DTMs).
RA-5	RA-5 (e)	CCI-002376	The organization defines the personnel or roles whom the information obtained from the vulnerability scanning process and security control assessments will be shared.	DoD has defined the personnel or roles as at a minimum, the ISSO and ISSM.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as at a minimum, the ISSO and ISSM.
RA-5	RA-5 (e)	CCI-001061	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).	The organization being inspected/assessed documents and implements a process to share information obtained from the vulnerability scanning process and security control assessments with at a minimum, the ISSM and ISSO to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies). DoD has defined the personnel or roles as at a minimum, the ISSO and ISSM.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed shares information obtained from the vulnerability scanning process and security control assessments with at a minimum, the ISSM and ISSO to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies). DoD has defined the personnel or roles as at a minimum, the ISSO and ISSM.
RA-5 (1)	RA-5 (1)	CCI-001062	The organization employs vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned.	The organization being inspected/assessed will employ scanning tools that maintain currency with industry standard information system vulnerabilities to ensure that scanning activities are conducted with the most up to date list of known vulnerabilities to include USCYBERCOM issued IAVMs. DoD has provided an enterprise scanning tool that fully meets this requirement. Organizations that choose not to use the enterprise scanning tool must identify which scanning tool they are using and ensure that it meets these requirements.	The organization conducting the inspection/assessment will: 1. If the inspected organization is using the DoD provided enterprise scanning tool, compliance with this control is complete. 2. Validate the identified tool in use by the inspected organization is able to maintain current up to date information system vulnerability data.
RA-5 (2)	RA-5 (2)	CCI-001063	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.	The organization being inspected/assessed will update the list of information system vulnerabilities scanned for prior to running scans. The organization must maintain a record of scans including the list of vulnerabilities scanned for. DoD has defined the frequency as prior to running scans.	The organization conducting the inspection/assessment obtains and examines the record of scans to ensure the latest most up to date scanning policies are present.
RA-5 (2)	RA-5 (2)	CCI-001064	The organization defines a frequency for updating the information system vulnerabilities scanned.	DoD has defined the frequency as prior to running scans.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as prior to running scans.
RA-5 (4)	RA-5 (4)	CCI-001066	The organization determines what information about the information system is discoverable by adversaries.	If the organization being inspected/assessed is conducting vulnerability scans IAW base control RA-5, they are compliant with this control.	The organization conducting the inspection/assessment will review results of validation of base control RA-5, if the inspected organization is compliant with the requirements of RA-5, they are compliant with this control.
RA-5 (4)	RA-5 (4)	CCI-002374	The organization defines the corrective actions when information about the information system is discoverable by adversaries.	The organization being inspected/assessed defines and documents the corrective actions when information about the information system is discoverable by adversaries. DoD has determined the corrective actions are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented corrective actions to ensure the organization being inspected/assessed defines the corrective actions when information about the information system is discoverable by adversaries. DoD has determined the corrective actions are not appropriate to define at the Enterprise level.
RA-5 (4)	RA-5 (4)	CCI-002375	The organization takes organization-defined corrective actions when information about the information system is discoverable by adversaries.	The organization being inspected/assessed documents and implements a process to take the corrective actions defined in RA-5 (4), CCI 2374 when information about the information system is discoverable by adversaries. The organization must maintain a record of actions taken.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of actions taken to ensure the organization being inspected/assessed takes the corrective actions defined in RA-5 (4), CCI 2374 when information about the information system is discoverable by adversaries.

RA-5 (5)	RA-5 (5)	CCI-001067	The information system implements privileged access authorization to organization-identified information system components for selected organization-defined vulnerability scanning activities.	The organization being inspected/assessed configures the information system to implement privileged access authorization to all information systems and infrastructure components for selected vulnerability scanning activities defined in RA-5 (5), CCI 2906. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1067. DoD has defined the information system components as all information systems and infrastructure components.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement privileged access authorization to all information systems and infrastructure components for selected vulnerability scanning activities defined in RA-5 (5), CCI 2906. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1067. DoD has defined the information system components as all information systems and infrastructure components.
RA-5 (5)	RA-5 (5)	CCI-001645	The organization identifies the information system components to which privileged access is authorized for selected organization-defined vulnerability scanning activities.	DoD has defined the information system components as all information systems and infrastructure components.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the information system components as all information systems and infrastructure components.
RA-5 (5)	RA-5 (5)	CCI-002906	The organization defines the vulnerability scanning activities in which the information system implements privileged access authorization to organization-identified information system components.	The organization being inspected/assessed defines and documents the vulnerability scanning activities in which the information system implements privileged access authorization to organization-identified information system components. DoD has determined the vulnerability scanning activities are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented vulnerability scanning activities to ensure the organization being inspected/assessed defines the vulnerability scanning activities in which the information system implements privileged access authorization to organization-identified information system components. DoD has determined the vulnerability scanning activities are not appropriate to define at the Enterprise level.
SA-1	SA-1 (a)	CCI-003089	The organization defines the personnel or roles to whom the system and services acquisition policy is disseminated.	DoD has defined the personnel or roles as all personnel.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as all personnel.
SA-1	SA-1 (a)	CCI-003090	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.	DoD has defined the personnel or roles as all personnel.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as all personnel.
SA-1	SA-1 (a) (1)	CCI-000602	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.	DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1 meet the DoD requirements for system and services acquisition policy and procedures. DoD Components are automatically compliant with this control because they are covered by the DoD level policies, DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1.	DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1 meet the DoD requirements for system and services acquisition policy and procedures. DoD Components are automatically compliant with this control because they are covered by the DoD level policies, DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1.
SA-1	SA-1 (a) (1)	CCI-000603	The organization disseminates to organization-defined personnel or roles a system and services acquisition policy.	DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1 meet the DoD requirements for system and services acquisition policy and procedures. DoD Components are automatically compliant with this control because they are covered by the DoD level policies, DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1.	DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1 meet the DoD requirements for system and services acquisition policy and procedures. DoD Components are automatically compliant with this control because they are covered by the DoD level policies, DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1.
SA-1	SA-1 (a) (2)	CCI-000605	The organization develops and documents procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.	DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1 meet the DoD requirements for system and services acquisition policy and procedures. DoD Components are automatically compliant with this control because they are covered by the DoD level policies, DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1.	DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1 meet the DoD requirements for system and services acquisition policy and procedures. DoD Components are automatically compliant with this control because they are covered by the DoD level policies, DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1.
SA-1	SA-1 (a) (2)	CCI-000606	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.	DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1 meet the DoD requirements for system and services acquisition policy and procedures. DoD Components are automatically compliant with this control because they are covered by the DoD level policies, DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1.	DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1 meet the DoD requirements for system and services acquisition policy and procedures. DoD Components are automatically compliant with this control because they are covered by the DoD level policies, DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1.

SA-1	SA-1 (b) (1)	CCI-000601	The organization defines the frequency to review and update the current system and services acquisition policy.	DoD has defined the frequency as every 5 years.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every 5 years.
SA-1	SA-1 (b) (1)	CCI-000604	The organization reviews and updates the current system and services acquisition policy in accordance with organization-defined frequency.	DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1 meet the DoD requirements for system and services acquisition policy and procedures. DoD Components are automatically compliant with this control because they are covered by the DoD level policies, DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1.	DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1 meet the DoD requirements for system and services acquisition policy and procedures. DoD Components are automatically compliant with this control because they are covered by the DoD level policies, DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1.
SA-1	SA-1 (b) (2)	CCI-001646	The organization defines the frequency to review and update the current system and services acquisition procedures.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.
SA-1	SA-1 (b) (2)	CCI-000607	The organization reviews and updates the current system and services acquisition procedures in accordance with organization-defined frequency.	DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1 meet the DoD requirements for system and services acquisition policy and procedures. DoD Components are automatically compliant with this control because they are covered by the DoD level policies, DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1.	DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1 meet the DoD requirements for system and services acquisition policy and procedures. DoD Components are automatically compliant with this control because they are covered by the DoD level policies, DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1.
SA-2	SA-2 (a)	CCI-003091	The organization determines information security requirements for the information system or information system service in mission/business process planning.	The organization being inspected/assessed determines and documents information security requirements for the information system or information system service in mission/business process planning.	The organization conducting the inspection/assessment obtains and examines the documented information security requirements to ensure the organization being inspected/assessed determines information security requirements for the information system or information system service in mission/business process planning.
SA-2	SA-2 (b)	CCI-000610	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.	The organization being inspected/assessed determines the resources (funding, staffing, etc.) required for the cybersecurity requirements to protect the information system or information system service as part of its planning, programming, and budget process (PPBE).	The organization conducting the inspection/assessment obtains and examines the planning, programming, and budget documentation to ensure the organization being inspected/assessed has determined the resources required for cybersecurity requirements to protect the information system or information system service.
SA-2	SA-2 (b)	CCI-000611	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.	The organization being inspected/assessed documents the resources (funding, staffing, etc.) required for the cybersecurity requirements to protect the information system or information system service as part of its planning, programming, and budget process (PPBE).	The organization conducting the inspection/assessment obtains and examines the planning, programming, and budget documentation to ensure the organization being inspected/assessed has documented the resources required for cybersecurity requirements to protect the information system or information system service.
SA-2	SA-2 (b)	CCI-000612	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.	The organization being inspected/assessed allocates the resources (funding, staffing, etc.) required for the cybersecurity requirements to protect the information system or information system service as part of its planning, programming, and budget process (PPBE).	The organization conducting the inspection/assessment obtains and examines the planning, programming, and budget documentation to ensure the organization being inspected/assessed has allocated the resources required for cybersecurity requirements to protect the information system or information system service.
SA-2	SA-2 (c)	CCI-000613	The organization establishes a discrete line item for information security in organizational programming documentation.	The organization being inspected/assessed identifies and establishes an individual line item for cybersecurity requirements to protect the information system as part of the planning, programming, and budget process (PPBE).	The organization conducting the inspection/assessment obtains and examines the planning, programming, and budget documentation to ensure the organization being inspected/assessed has identified and established an individual line item for cybersecurity requirements to protect the information system.
SA-2	SA-2 (c)	CCI-000614	The organization establishes a discrete line item for information security in organizational budgeting documentation.	The organization being inspected/assessed identifies and establishes an individual line item for cybersecurity requirements to protect the information system as part of the planning, programming, and budget process (PPBE).	The organization conducting the inspection/assessment obtains and examines the planning, programming, and budget documentation to ensure the organization being inspected/assessed has identified and established an individual line item for cybersecurity requirements to protect the information system.
SA-3	SA-3 (a)	CCI-003092	The organization defines a system development life cycle that is used to manage the information system.	The organization being inspected/assessed defines and documents a system development life cycle that is used to manage the information system. DoD has determined the system development life cycle is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented system development life cycle to ensure the organization being inspected/assessed defines a system development life cycle that is used to manage the information system. DoD has determined the system development life cycle is not appropriate to define at the Enterprise level.

SA-3	SA-3 (a)	CCI-000615	The organization manages the information system using organization-defined system development life cycle that incorporates information security considerations.	The organization being inspected/assessed documents and implements a process to manage the information system using the system development life cycle defined in SA-3, CCI 3092 that incorporates information security considerations IAW DoDI 8580.1.	The organization conducting the inspection/assessment obtains and examines the documented process and artifacts of the system development life cycle process to ensure the organization being inspected/assessed manages the information system using the system development life cycle defined in SA-3, CCI 3092 that incorporates information security considerations IAW DoDI 8580.1.
SA-3	SA-3 (b)	CCI-000616	The organization defines and documents information system security roles and responsibilities throughout the system development life cycle.	The organization being inspected/assessed defines and documents information system security roles and responsibilities throughout the system development life cycle IAW DoDI 8580.1 .	The organization conducting the inspection/assessment obtains and examines the information system security roles and responsibilities to ensure the organization being inspected/assessed defines and documents information system security roles and responsibilities throughout the system development life cycle IAW DoDI 8580.1.
SA-3	SA-3 (c)	CCI-000618	The organization identifies individuals having information system security roles and responsibilities.	The organization being inspected/assessed identifies and documents individuals having information system security roles and responsibilities.	The organization conducting the inspection/assessment obtains and examines the documented individuals having information system security roles and responsibilities to ensure the organization being inspected/assessed identifies individuals having information system security roles and responsibilities.
SA-3	SA-3 (d)	CCI-003093	The organization integrates the organizational information security risk management process into system development life cycle activities.	The organization being inspected/assessed documents and implements a process to integrate the organizational information security risk management process into system development life cycle activities.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed integrates the organizational information security risk management process into system development life cycle activities.
SA-4	SA-4 (a)	CCI-003094	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.	The organization being inspected/assessed documents within contracts/agreements for the information system, system component, or information system service, the security functional requirements, explicitly or by reference, IAW DoDI 8580.1.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed 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 including DoDI 8580.1.
SA-4	SA-4 (b)	CCI-003095	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.	The organization being inspected/assessed documents within contracts/agreements for the information system, system component, or information system service, the security strength requirements, explicitly or by reference, IAW DoDI 8580.1.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed 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 including DoDI 8580.1.
SA-4	SA-4 (c)	CCI-003096	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.	The organization being inspected/assessed documents within contracts/agreements for the information system, system component, or information system service, the security assurance requirements, explicitly or by reference, IAW DoDI 8580.1.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed 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 including DoDI 8580.1.
SA-4	SA-4 (d)	CCI-003097	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.	The organization being inspected/assessed documents within contracts/agreements for the information system, system component, or information system service, the security-related documentation requirements, explicitly or by reference.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed 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.
SA-4	SA-4 (e)	CCI-003098	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.	The organization being inspected/assessed documents within contracts/agreements for the information system, system component, or information system service, requirements for protecting security-related documentation, explicitly or by reference.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed 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.

SA-4	SA-4 (f)	CCI-003099	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.	The organization being inspected/assessed documents within contracts/agreements for the information system, system component, or information system service, a description of the information system development environment and environment in which the system is intended to operate, explicitly or by reference.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed includes a 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.
SA-4	SA-4 (g)	CCI-003100	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.	The organization being inspected/assessed documents within contracts/agreements for the information system, system component, or information system service, acceptance criteria, explicitly or by reference.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed 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.
SA-4 (7)	SA-4 (7) (a)	CCI-000634	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.	The organization being inspected/assessed, when using commercially provided IA and IA-enabled IT products uses only 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.	The organization conducting the inspection/assessment obtains and examines the hardware and software lists to ensure the organization being inspected/assessed, when using commercially provided IA and IA-enabled IT products uses only 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.
SA-4 (7)	SA-4 (7) (b)	CCI-000635	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.	The organization being inspected/assessed, when using commercially provided IA or IA enabled IT products for which there is no NIAP-approved protection profile, relies on FIPS-validated cryptographic modules.	The organization conducting the inspection/assessment obtains and examines the hardware and software lists to ensure the organization being inspected/assessed, when using commercially provided IA or IA enabled IT products for which there is no NIAP-approved protection profile, relies on FIPS-validated cryptographic modules.
SA-4 (9)	SA-4 (9)	CCI-003114	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.	The organization being inspected/assessed documents within contracts/agreements, the requirement that the developer of the information system, system component, or information system service identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use. Ports identified shall be assessed and planned for in light of DISA's PPSM requirements.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use.
SA-4 (10)	SA-4 (10)	CCI-003116	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.	The organization being inspected/assessed employs DoD approved PKI tokens for identity verification.	The organization conducting the inspection/assessment examines the information system to ensure DoD approved PKI tokens are implemented for identity verification.
SA-5	SA-5 (a) (1)	CCI-003124	The organization obtains administrator documentation for the information system, system component, or information system services that describes secure configuration of the system, component, or service.	The organization being inspected/assessed documents within contracts/agreements, requirements that the developer provide administrator documentation for the information system, system component or information system service that describe secure configuration of the system, component, or service.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer provide administrator documentation for the information system, system component or information system service that describe secure configuration of the system, component, or service.
SA-5	SA-5 (a) (1)	CCI-003125	The organization obtains administrator documentation for the information system, system component, or information system services that describes secure installation of the system, component, or service.	The organization being inspected/assessed documents within contracts/agreements, requirements that the developer provide administrator documentation for the information system, system component or information system service that describe secure installation of the system, component, or service.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer provide administrator documentation for the information system, system component or information system service that describe secure installation of the system, component, or service.
SA-5	SA-5 (a) (1)	CCI-003126	The organization obtains administrator documentation for the information system, system component, or information system services that describes secure operation of the system, component, or service.	The organization being inspected/assessed documents within contracts/agreements, requirements that the developer provide administrator documentation for the information system, system component or information system service that describe secure operation of the system, component, or service.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer provide administrator documentation for the information system, system component or information system service that describe secure operation of the system, component, or service.

SA-5	SA-5 (a) (2)	CCI-003127	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.	The organization being inspected/assessed documents within contracts/agreements, requirements that the developer provide administrator documentation for the information system, system component or information system service that describe effective use and maintenance of security functions/mechanisms.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer provide administrator documentation for the information system, system component or information system service that describe effective use and maintenance of security functions/mechanisms.
SA-5	SA-5 (a) (3)	CCI-003128	The organization obtains administrator documentation for the information system, system component, or information system services that describes known vulnerabilities regarding configuration and use of administrative (i.e. privileged) functions.	The organization being inspected/assessed documents within contracts/agreements, requirements that the developer provide administrator documentation for the information system, system component or information system service that describe known vulnerabilities regarding configuration and use of administrative (i.e. privileged) functions.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer provide administrator documentation for the information system, system component or information system service that describe known vulnerabilities regarding configuration and use of administrative (i.e. privileged) functions.
SA-5	SA-5 (b) (1)	CCI-003129	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.	The organization being inspected/assessed documents within contracts/agreements, requirements that the developer provide 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.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer provide 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.
SA-5	SA-5 (b) (2)	CCI-003130	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.	The organization being inspected/assessed documents within contracts/agreements, requirements that the developer provide 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.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer provide 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.
SA-5	SA-5 (b) (3)	CCI-003131	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.	The organization being inspected/assessed documents within contracts/agreements, requirements that the developer provide 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.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer provide 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.
SA-5	SA-5 (c)	CCI-000642	The organization documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent.	The organization being inspected/assessed documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent.	The organization conducting the inspection/assessment obtains and examines the documented attempts to ensure the organization being inspected/assessed documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent.
SA-5	SA-5 (c)	CCI-003132	The organization takes organization-defined actions in response to attempts to obtain either unavailable or nonexistent documentation for information system, system component, or information system service.	The organization being inspected/assessed takes actions defined in SA-5, CCI 3133 in response to attempts to obtain either unavailable or nonexistent documentation for information system, system component, or information system service. The organization must maintain a record of actions taken. DoD has determined the actions are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the record of actions taken to ensure the organization being inspected/assessed takes actions defined in SA-5, CCI 3133 in response to attempts to obtain either unavailable or nonexistent documentation for information system, system component, or information system service. DoD has determined the actions are not appropriate to define at the Enterprise level.
SA-5	SA-5 (c)	CCI-003133	The organization defines actions to be taken in response to attempts to obtain either unavailable or nonexistent documentation for information system, system component, or information system service.	The organization being inspected/assessed defines and documents actions to be taken in response to attempts to obtain either unavailable or nonexistent documentation for information system, system component, or information system service. DoD has determined the actions are not appropriate to define at the Enterprise level.	The organization conducting inspection/assessment obtains and examines the documented actions to ensure the organization being inspected/assessed defines action to be taken in response to attempts to obtain either unavailable or nonexistent documentation for information system, system component, or information system service. DoD has determined the actions are not appropriate to define at the Enterprise level.

SA-5	SA-5 (d)	CCI-003134	The organization protects information system, system component, or information system service documentation as required, in accordance with the risk management strategy.	The organization being inspected/assessed documents and implements processes to store and handle information system, system component, or information system service documentation as required, in accordance with the risk management strategy.	The organization conducting the inspection/assessment obtains and examines the documented processes to ensure the organization being inspected/assessed stores and handles information system, system component, or information system service documentation as required, in accordance with the risk management strategy.
SA-5	SA-5 (e)	CCI-003135	The organization distributes information system, system component, or information system service documentation to organization-defined personnel or roles.	The organization being inspected/assessed distributes information system, system component, or information system service documentation to at a minimum, the ISSO, ISSM, and SCA, via an information sharing capability. DoD has defined the personnel or roles as at a minimum, the ISSO, ISSM, and SCA.	The organization conducting the inspection/assessment obtains and examines the information system, system component, or information system service documentation via the organization's information sharing capability to ensure the organization being inspected/assessed distributes information system, system component, or information system service documentation to at a minimum, the ISSO, ISSM, and SCA. DoD has defined the personnel or roles as at a minimum, the ISSO, ISSM, and SCA.
SA-5	SA-5 (e)	CCI-003136	The organization defines the personnel or roles the information system, system component, or information system service documentation is to be distributed.	DoD has defined the personnel or roles as at a minimum, the ISSO, ISSM, and SCA.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as at a minimum, the ISSO, ISSM, and SCA.
SA-8	SA-8	CCI-000664	The organization applies information system security engineering principles in the specification of the information system.	The organization managing the acquisition/development of the information system (e.g. PM) applies and documents system security engineering (SSE) principles as part of the overall systems engineering process IAW DoDD 5000.01 and DoDI 5000.02. The primary source of general and DoD-specific guidance on SSE can be found in the NIST SP 800-160 - Systems Security Engineering, currently in draft form, and can be found here: http://csrc.nist.gov/publications/PubsSPs.html. Additional guidance can be found in the Defense Acquisition Guidebook (DAG) Chapters 4 and 13, found here: https://dag.dau.mil/. This CCI does not apply to COTS products. The organization managing the acquisition/development of the information system must ensure that the system requirements documents reflect the system security engineering principles that can be applied to information systems in development, systems undergoing major upgrades and to the extent feasible	The organization conducting the inspection/assessment obtains and examines the system requirements documents to ensure that the organization being inspected/assessed applies information system security engineering principles in the specification of the information system.
SA-8	SA-8	CCI-000665	The organization applies information system security engineering principles in the design of the information system.	The organization managing the acquisition/development of the information system (e.g. PM) applies and documents system security engineering (SSE) principles as part of the overall systems engineering process IAW DoDD 5000.01 and DoDI 5000.02. The primary source of general and DoD-specific guidance on SSE can be found in the NIST SP 800-160 - Systems Security Engineering, currently in draft form, and can be found here: http://csrc.nist.gov/publications/PubsSPs.html. Additional guidance can be found in the Defense Acquisition Guidebook (DAG) Chapters 4 and 13, found here: https://dag.dau.mil/. This CCI does not apply to COTS products. The organization managing the acquisition/development of the information system must ensure that the design documents reflect the system security engineering principles that can be applied to information systems in development, systems undergoing major upgrades and to the extent feasible systems in	The organization conducting the inspection/assessment obtains and examines the design documents to ensure that the organization being inspected/assessed applies information system security engineering principles in the design of the information system.

SA-8	SA-8	CCI-000666	The organization applies information system security engineering principles in the development of the information system.	The organization managing the acquisition/development of the information system (e.g. PM) applies and documents system security engineering (SSE) principles as part of the overall systems engineering process IAW DoDD 5000.01 and DoDI 5000.02. The primary source of general and DoD-specific guidance on SSE can be found in the NIST SP 800-160 - Systems Security Engineering, currently in draft form, and can be found here: http://csrc.nist.gov/publications/PubsSPs.html. Additional guidance can be found in the Defense Acquisition Guidebook (DAG) Chapters 4 and 13, found here: https://dag.dau.mil/. This CCI does not apply to COTS products. The organization managing the acquisition/development of the information system must ensure that the development procedures reflect the system security engineering principles that can be applied to information systems in development, systems undergoing major upgrades and to the extent feasible systems in	The organization conducting the inspection/assessment obtains and examines the system development procedures (e.g. configuration management plans, code review procedures, and coding style guides) to ensure that the organization being inspected/assessed applies information system security engineering principles in the development of the information system.
SA-8	SA-8	CCI-000667	The organization applies information system security engineering principles in the implementation of the information system.	The organization managing the acquisition/development of the information system (e.g. PM) applies and documents system security engineering (SSE) principles as part of the overall systems engineering process IAW DoDD 5000.01 and DoDI 5000.02. The primary source of general and DoD-specific guidance on SSE can be found in the NIST SP 800-160 - Systems Security Engineering, currently in draft form, and can be found here: http://csrc.nist.gov/publications/PubsSPs.html. Additional guidance can be found in the Defense Acquisition Guidebook (DAG) Chapters 4 and 13, found here: https://dag.dau.mil/. This CCI does not apply to COTS products. The organization managing the acquisition/development of the information system must employ the procedures identified in SA-8, CCI, 000666 during the implementation of the information system. The system owner must maintain an audit trail of the activities conducted IAW SA-8, CCI 000666. An example of artifacts is	The organization conducting the inspection/assessment obtains and examines the audit trail artifacts that were created during the implementation of SA-8, CCI 000666 to ensure that the organization being inspected/assessed applies information system security engineering principles in the implementation of the information system and that changes are made IAW the configuration management plan (CM-9, CCI 001790).
SA-8	SA-8	CCI-000668	The organization applies information system security engineering principles in the modification of the information system.	The organization managing the acquisition/development of the information system (e.g. PM) applies and documents system security engineering (SSE) principles as part of the overall systems engineering process IAW DoDD 5000.01 and DoDI 5000.02. The primary source of general and DoD-specific guidance on SSE can be found in the NIST SP 800-160 - Systems Security Engineering, currently in draft form, and can be found here: http://csrc.nist.gov/publications/PubsSPs.html. Additional guidance can be found in the Defense Acquisition Guidebook (DAG) Chapters 4 and 13, found here: https://dag.dau.mil/. This CCI does not apply to COTS products. The organization managing the acquisition/development of the information system must employ the procedures identified in SA-8, CCI, 000666 during the modification of the information system. The system owner must maintain an audit trail of the activities conducted IAW SA-8, CCI 000666. An example of artifacts is	The organization conducting the inspection/assessment obtains and examines the audit trail artifacts that were created during the modification of SA-8, CCI 000666 to ensure that the organization being inspected/assessed applies information system security engineering principles in the modification of the information system and that changes are made IAW the configuration management plan (CM-9, CCI 001790).
SA-9	SA-9 (a)	CCI-003137	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.	DoD has defined the security controls as security controls defined by CNSSI 1253.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the security controls as security controls defined by CNSSI 1253.

SA-9	SA-9 (a)	CCI-000669	The organization requires that providers of external information system services comply with organizational information security requirements.	The organization being inspected/assessed documents within contracts/agreements, requirements that providers of external information system services comply with any organization-specific information security requirements.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that providers of external information system services comply with any organization-specific information security requirements.
SA-9	SA-9 (a)	CCI-000670	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.	The organization being inspected/assessed documents within contracts/agreements, the requirement that providers of external information system services employ security controls defined in CNSSI 1253. DoD has defined the security controls as security controls defined by CNSSI 1253.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that providers of external information system services employ security controls defined in CNSSI 1253. DoD has defined the security controls as security controls defined by CNSSI 1253.
SA-9	SA-9 (b)	CCI-000671	The organization defines government oversight with regard to external information system services.	The organization being inspected/assessed must define in the official documentation governing the provision of the external IT services (e.g. contract, MOU, MOA, SLA, etc.) the government oversight to be conducted on external information system services and service provider.	The organization conducting the inspection/assessment obtains and examines the official documentation governing the provision of the external IT services (e.g. contract, MOU, MOA, SLA, etc.) to confirm the organization has clearly defined the government oversight to be conducted on external information system services and service providers.
SA-9	SA-9 (b)	CCI-000672	The organization documents government oversight with regard to external information system services.	The organization being inspected/assessed must establish in the official documentation governing the provision of the external IT services (e.g. contract, MOU, MOA, SLA, etc.) the government oversight to be conducted on external information system services and service provider.	The organization conducting the inspection/assessment obtains and examines the official documentation governing the provision of the external IT services (e.g. contract, MOU, MOA, SLA, etc.) to confirm the organization has clearly established the government oversight to be conducted on external information system services and service providers.
SA-9	SA-9 (b)	CCI-000673	The organization defines user roles and responsibilities with regard to external information system services.	The organization being inspected/assessed must define in the official documentation governing the provision of the external IT services (e.g. contract, MOU, MOA, SLA, etc.) the roles and responsibilities of all types of users of the external information system services.	The organization conducting the inspection/assessment obtains and examines the official documentation governing the provision of the external IT services (e.g. contract, MOU, MOA, SLA, etc.) to confirm the organization has clearly defined the roles and responsibilities of all types of users of the external information system services.
SA-9	SA-9 (b)	CCI-000674	The organization documents user roles and responsibilities with regard to external information system services.	The organization being inspected/assessed must establish in the official documentation governing the provision of the external IT services (e.g. contract, MOU, MOA, SLA, etc.) the roles and responsibilities of all types of users of the external information system services.	The organization conducting the inspection/assessment obtains and examines the official documentation governing the provision of the external IT services (e.g. contract, MOU, MOA, SLA, etc.) to confirm the organization has clearly established the roles and responsibilities of all types of users of the external information system services.
SA-9	SA-9 (c)	CCI-003138	The organization employs organization-defined processes, methods, and techniques to monitor security control compliance by external service providers on an ongoing basis.	The organization being inspected/assessed implements the processes, methods, and techniques defined in SA-9, CCI 3139 to monitor security control compliance by external service providers on an ongoing basis. The organization must maintain records of monitoring.	The organization conducting the inspection/assessment obtains and examines the records of monitoring to ensure the organization being inspected/assessed implements the processes, methods, and techniques defined in SA-9, CCI 3139 to monitor security control compliance by external service providers on an ongoing basis.
SA-9	SA-9 (c)	CCI-003139	The organization defines processes, methods, and techniques to employ to monitor security control compliance by external service providers on an ongoing basis.	The organization being inspected/assessed defines and documents processes, methods, and techniques to employ to monitor security control compliance by external service providers on an ongoing basis. DoD has determined the processes, methods, and techniques are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented processes, methods, and techniques to ensure the organization being inspected/assessed defines processes, methods, and techniques to employ to monitor security control compliance by external service providers on an ongoing basis.
SA-9 (1)	SA-9 (1) (a)	CCI-003140	The organization conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services.	The organization being inspected/assessed documents and implements a process to conduct an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services. The organization must maintain a record of risk assessment.	The organization conducting the inspection/assessment obtains and examines a list of acquired or outsourced information security services and the record of risk assessment to ensure the organization being inspected/assessed conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services.

SA-9 (1)	SA-9 (1) (b)	CCI-003141	The organization ensures that the acquisition or outsourcing of dedicated information security services is approved by organization-defined personnel or roles.	The organization being inspected/assessed ensures that the acquisition or outsourcing of dedicated information security services is approved by the DoD Component CIO or their delegate(s). The organization must maintain a record of approvals. DoD has defined the personnel or roles the DoD Component CIO or their delegate(s).	The organization conducting the inspection/assessment obtains and examines a list of acquired or outsourced information security services as well as the record of approvals to ensure the organization being inspected/assessed ensures that the acquisition or outsourcing of dedicated information security services is approved by the DoD Component CIO or their delegate(s). DoD has defined the personnel or roles the DoD Component CIO or their delegate(s).
SA-9 (1)	SA-9 (1) (b)	CCI-003142	The organization defines the personnel or roles authorized to approve the acquisition or outsourcing of dedicated information security services.	DoD has defined the personnel or roles the DoD Component CIO or their delegate(s).	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles the DoD Component CIO or their delegate(s).
SA-9 (2)	SA-9 (2)	CCI-003143	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.	The organization being inspected/assessed documents within contracts/agreements, the requirement that providers of all external information system services identify the functions, ports, protocols, and other services required for the use of such services. DoD has defined the external information system services as all external information system services.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that providers of all external information system services identify the functions, ports, protocols, and other services required for the use of such services. DoD has defined the external information system services as all external information system services.
SA-9 (2)	SA-9 (2)	CCI-003144	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.	DoD has defined the external information system services as all external information system services.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the external information system services as all external information system services.
SA-10	SA-10 (a)	CCI-003155	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.	The organization being inspected/assessed requires within contracts/agreements that the developer of the information system, system component, or information system service perform configuration management during system, component or service design, development, implementation and/or operation. The configuration management process applies to: 1. Documentation developed or used in the lifecycle, including requirements and interface specifications; 2. Elements including design libraries; 3. Tools including design tools and test tools; 4. Technical data including test data; and 5. Information on element and system lifecycle processes	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires the developer of the information system, system component, or information system service perform configuration management during system, component or service design, development, implementation and/or operation.
SA-10	SA-10 (b)	CCI-003156	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.	The organization being inspected/assessed requires within contracts/agreements that the developer of the information system, system component, or information system service document the integrity of changes to configuration items under configuration management defined in SA-10, CCI 3159.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service document the integrity of changes to configuration items under configuration management defined in SA-10, CCI 3159.
SA-10	SA-10 (b)	CCI-003157	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.	The organization being inspected/assessed requires within contracts/agreements the requirement that the developer of the information system, system component, or information system service manage the integrity of changes to configuration items under configuration management defined in SA-10, CCI 3159.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service manage the integrity of changes to configuration items under configuration management defined in SA-10, CCI 3159.
SA-10	SA-10 (b)	CCI-003158	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.	The organization being inspected/assessed requires within contracts/agreements that the developer of the information system, system component, or information system service control the integrity of changes to configuration items under configuration management defined in SA-10, CCI 3159.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service control the integrity of changes to configuration items under configuration management defined in SA-10, CCI 3159.

SA-10	SA-10 (b)	CCI-003159	The organization defines the configuration items under configuration management that require the integrity of changes to be documented, managed and controlled.	The organization being inspected/assessed defines and documents the configuration items under configuration management that require the integrity of changes to be documented, managed and controlled. DoD has determined the configuration items are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented configuration items to ensure the organization being inspected/assessed defines the configuration items under configuration management that require the integrity of changes to be documented, managed and controlled. DoD has determined the configuration items are not appropriate to define at the Enterprise level.
SA-10	SA-10 (c)	CCI-000692	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.	The organization being inspected/assessed requires within contracts/agreements that the developer of the information system, system component, or information system service implement only organization-approved changes to the system, component, or service throughout its life cycle.	The organization conducting the inspection/assessment obtains and examines contracts/agreements between the organization and the IS developer to confirm the organization has established in its acquisition contracts/agreements the requirement that the IS developer implement only organization-approved changes to the system, component, or service throughout its life cycle.
SA-10	SA-10 (d)	CCI-000694	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.	The organization being inspected/assessed requires within contracts/agreements that the developer of the information system, system component, or information system service document approved changes to the system, component, or service.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service document approved changes to the system, component, or service.
SA-10	SA-10 (d)	CCI-003160	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.	The organization being inspected/assessed requires within contracts/agreements that the developer of the information system, system component, or information system service document the potential security impacts of approved changes to the system, component, or service.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service document the potential security impacts of approved changes to the system, component, or service.
SA-10	SA-10 (e)	CCI-003161	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.	The organization being inspected/assessed requires within contracts/agreements that the developer of the information system, system component, or information system service track security flaws within the system, component, or service.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service track security flaws within the system, component, or service.
SA-10	SA-10 (e)	CCI-003162	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.	The organization being inspected/assessed requires within contracts/agreements that the developer of the information system, system component, or information system service track flaw resolution within the system, component, or service.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service track flaw resolution within the system, component, or service.
SA-10	SA-10 (e)	CCI-003163	The organization requires the developer of the information system, system component, or information system service to report security flaws and flaw resolution within the system, component, or service findings to organization-defined personnel.	The organization being inspected/assessed requires within contracts/agreements that the developer of the information system, system component, or information system service report security flaws and flaw resolution within the system, component, or service findings to at a minimum, the ISSO and ISSM. DoD has defined the personnel as at a minimum, the ISSO and ISSM.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service report security flaws and flaw resolution within the system, component, or service findings to at a minimum, the ISSO and ISSM. DoD has defined the personnel as at a minimum, the ISSO and ISSM.
SA-10	SA-10 (e)	CCI-003164	The organization defines the personnel to whom security flaw findings and flaw resolution within the system, component, or service are reported.	DoD has defined the personnel as at a minimum, the ISSO and ISSM.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel as at a minimum, the ISSO and ISSM.

SA-10 (1)	SA-10 (1)	CCI-000698	The organization requires the developer of the information system, system component, or information system service to enable integrity verification of software and firmware components.	The organization being inspected/assessed requires within contracts/agreements that the developer of the information system, system component, or information system service enable integrity verification of software and firmware components. The organization being inspected/assessed requires the developer to enable integrity verification of software and firmware that may include: 1. Stipulating and monitoring logical delivery of products and services, requiring downloading from approved, verification-enhanced sites; 2. Encrypting elements (software, software patches, etc.) and supply chain process data in transit (motion) and at rest throughout delivery; 3. Requiring suppliers to provide their elements “secure by default”, so that additional configuration is required to make the element insecure; 4. Implementing software designs using programming languages and tools that reduce the likelihood of weaknesses; 5. Implementing cryptographic hash verification; and	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service enable integrity verification of software and firmware components.
SA-12	SA-12	CCI-000722	The organization defines the security safeguards to employ to protect against supply chain threats to the information system, system component, or information system service.	DoD has defined the requirements to protect against supply chain threats in DoDI 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)."	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the requirements to protect against supply chain threats in DoDI 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)."
SA-12	SA-12	CCI-000723	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.	The organization being inspected/assessed must identify and document in the Security Plan whether the system is a “covered system” IAW DoDI 5200.44. If it is a covered system, the organization must implement the requirements below: 1. Conduct a criticality analysis to identify mission critical functions and critical components and reduce the vulnerability of such functions and components through secure system design; 2. Request threat analysis of suppliers of critical components from the TSN focal point and manage access to and control of threat analysis products containing U.S. person information; 3. Engage TSN focal points for guidance on managing identified risk using DoD Components and Enterprise risk management resources; and 4. Apply TSN best practices, processes, techniques, and procurement tools prior to the acquisition of critical components or their integration into applicable systems, at any point in the system lifecycle. Such tools and practices include contract requirements and the SCRM key practices Guide.	The organization conducting the inspection/assessment obtains and examines the Security Plan for the system to determine whether the system is a “covered system” IAW DoDI 5200.44. If it is a covered system, the organization conducting the inspection/assessment obtains and examines documentation of compliance with DoDI 5200.44, to ensure the organization being inspected/assessed has: 1. Conducted a criticality analysis to identify mission critical functions and critical components and reduced the vulnerability of such functions and components through secure system design; 2. Requested threat analysis of suppliers of critical components from the TSN focal point and managed access to and control of threat analysis products containing U.S. person information; 3. Engaged TSN focal points for guidance on managing identified risk using DoD Components and Enterprise risk management resources; and 4. Applied TSN best practices, processes, techniques, and procurement tools prior to the acquisition of critical components or their integration into applicable systems, at any point in the system lifecycle. Such tools and practices include contract requirements and the SCRM key practices Guide.
SA-15	SA-15	CCI-003233	The organization requires the developer of the information system, system component, or information system service to follow a documented development process.	The organization being inspected/assessed requires within contracts/agreements that the developer of the information system, system component, or information system service to follow a documented development process.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service to follow a documented development process.
SA-15	SA-15 (a) (1)	CCI-003234	The documented information system, system component, or information system service development process explicitly addresses security requirements.	The organization being inspected/assessed requires within contracts/agreements that the developer of the information system, system component, or information system service explicitly addresses security requirements.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service explicitly addresses security requirements.
SA-15	SA-15 (a) (2)	CCI-003235	The documented information system, system component, or information system service development process identifies the standards used in the development process.	The organization being inspected/assessed requires within contracts/agreements that the developer of the information system, system component, or information system service identifies the standards used in the development process, for example, programming languages and computer-aided design (CAD) systems.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service identifies the standards used in the development process.

SA-15	SA-15 (a) (2)	CCI-003236	The documented information system, system component, or information system service development process identifies the tools used in the development process.	The organization being inspected/assessed requires within contracts/agreements that the developer of the information system, system component, or information system service identifies the tools used in the development process, for example, programming languages and computer-aided design (CAD) systems.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service identifies the tools used in the development process.
SA-15	SA-15 (a) (3)	CCI-003237	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.	The organization being inspected/assessed requires within contracts/agreements that the developer of the information system, system component, or information system service documents the specific tool options and tool configurations used in the development process.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service documents the specific tool options and tool configurations used in the development process.
SA-15	SA-15 (a) (4)	CCI-003238	The documented information system, system component, or information system service development process documents changes to the process and/or tools used in development.	The organization being inspected/assessed requires within contracts/agreements that the developer of the information system, system component, or information system service documents changes to the process and/or tools used in development.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service documents changes to the process and/or tools used in development.
SA-15	SA-15 (a) (4)	CCI-003239	The documented information system, system component, or information system service development process manages changes to the process and/or tools used in development.	The organization being inspected/assessed requires within contracts/agreements that the developer of the information system, system component, or information system service document a process to manage changes to the process and/or tools used in development.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service document a process to manage changes to the process and/or tools used in development.
SA-15	SA-15 (a) (4)	CCI-003240	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.	The organization being inspected/assessed requires within contracts/agreements that the developer of the information system, system component, or information system service document the integrity of changes to the process and/or tools used in development.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service document the integrity of changes to the process and/or tools used in development.
SA-15	SA-15 (b)	CCI-003241	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.	The organization being inspected/assessed documents and implements a process to review the development process before first use and annually thereafter to determine if the development process selected and employed can satisfy the security requirements defined in SA-15, CCI 3246. Reviews of development processes can include, for example, the use of capability maturity model integration (CMMI) to determine the potential effectiveness of such processes. The organization must maintain a record of reviews. DoD has defined the frequency as before first use and annually thereafter.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of reviews to ensure the organization being inspected/assessed reviews the development process before first use and annually thereafter to determine if the development process selected and employed can satisfy the security requirements defined in SA-15, CCI 3246. DoD has defined the frequency as before first use and annually thereafter.
SA-15	SA-15 (b)	CCI-003242	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.	The organization being inspected/assessed documents and implements a process to review the development standards before first use and annually thereafter to determine if the development standards selected and employed can satisfy the security requirements defined in SA-15, CCI 3246. The organization must maintain a record of reviews. DoD has defined the frequency as before first use and annually thereafter.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of reviews to ensure the organization being inspected/assessed reviews the development standards before first use and annually thereafter to determine if the development standards selected and employed can satisfy the security requirements defined in SA-15, CCI 3246. DoD has defined the frequency as before first use and annually thereafter.

SA-15	SA-15 (b)	CCI-003243	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.	The organization being inspected/assessed documents and implements a process to review the development tools before first use and annually thereafter to determine if the development tools selected and employed can satisfy the security requirements defined in SA-15, CCI 3246. The organization must maintain a record of reviews. DoD has defined the frequency as before first use and annually thereafter.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of reviews to ensure the organization being inspected/assessed reviews the development tools before first use and annually thereafter to determine if the development tools selected and employed can satisfy the security requirements defined in SA-15, CCI 3246. DoD has defined the frequency as before first use and annually thereafter.
SA-15	SA-15 (b)	CCI-003244	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.	The organization being inspected/assessed documents and implements a process to review the development tool options/configurations before first use and annually thereafter to determine if the development tool options/configurations selected and employed can satisfy the security requirements defined in SA-15, CCI 3246. The organization must maintain a record of reviews. DoD has defined the frequency as before first use and annually thereafter.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of reviews to ensure the organization being inspected/assessed reviews the development tool options/configurations before first use and annually thereafter to determine if the development tool options/configurations selected and employed can satisfy the security requirements defined in SA-15, CCI 3246. DoD has defined the frequency as before first use and annually thereafter.
SA-15	SA-15 (b)	CCI-003245	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.	DoD has defined the frequency as before first use and annually thereafter.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as before first use and annually thereafter.
SA-15	SA-15 (b)	CCI-003246	The organization defines the security requirements that must be satisfied by conducting a review of the development process, standards, tools, and tool options/configurations.	The organization being inspected/assessed defines and documents the security requirements that must be satisfied by conducting a review of the development process, standards, tools, and tool options/configurations. DoD has determined the security requirements are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented security requirements to ensure the organization being inspected/assessed defines the security requirements that must be satisfied by conducting a review of the development process, standards, tools, and tool options/configurations. DoD has determined the security requirements are not appropriate to define at the Enterprise level.
SA-15 (9)	SA-15 (9)	CCI-003283	The organization approves the use of live data in development environments for the information system, system component, or information system service.	The organization being inspected/assessed documents and implements a process to approve the use of live data in development environments for the information system, system component, or information system service. The organization must maintain a record of approvals.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of approvals to ensure the organization being inspected/assessed approves the use of live data in development environments for the information system, system component, or information system service.
SA-15 (9)	SA-15 (9)	CCI-003284	The organization approves the use of live data in test environments for the information system, system component, or information system service.	The organization being inspected/assessed documents and implements a process to approve the use of live data in test environments for the information system, system component, or information system service. The organization must maintain a record of approvals.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of approvals to ensure the organization being inspected/assessed approves the use of live data in test environments for the information system, system component, or information system service.
SA-15 (9)	SA-15 (9)	CCI-003285	The organization documents the use of live data in development environments for the information system, system component, or information system service.	The organization being inspected/assessed documents the use of live data in development environments for the information system, system component, or information system service.	The organization conducting the inspection/assessment obtains and examines the documented use of live data in test environments to ensure the organization being inspected/assessed documents the use of live data in development environments for the information system, system component, or information system service.
SA-15 (9)	SA-15 (9)	CCI-003286	The organization documents the use of live data in test environments for the information system, system component, or information system service.	The organization being inspected/assessed documents the use of live data in test environments for the information system, system component, or information system service.	The organization conducting the inspection/assessment obtains and examines the documented use of live data in test environments to ensure the organization being inspected/assessed documents the use of live data in test environments for the information system, system component, or information system service.

SA-15 (9)	SA-15 (9)	CCI-003287	The organization controls the use of live data in development environments for the information system, system component, or information system service.	The organization being inspected/assessed documents and implements a process to control the use of live data in development environments for the information system, system component, or information system service. The Enclave Test and Development STIG identifies requirements for test and development environments.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed controls the use of live data in development environments for the information system, system component, or information system service.
SA-15 (9)	SA-15 (9)	CCI-003288	The organization controls the use of live data in test environments for the information system, system component, or information system service.	The organization being inspected/assessed documents and implements a process to control the use of live data in test environments for the information system, system component, or information system service. The Enclave Test and Development STIG identifies requirements for test and development environments.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed controls the use of live data in test environments for the information system, system component, or information system service.
SA-19	SA-19 (a)	CCI-003356	The organization develops anti-counterfeit policy that include the means to detect counterfeit components from entering the information system.	The organization being inspected/assessed develops and documents an anti-counterfeit policy that include the means to detect counterfeit components from entering the information system.	The organization conducting the inspection/assessment obtains and examines the documented anti-counterfeit policy to ensure the organization being inspected/assessed develops an anti-counterfeit policy that include the means to detect counterfeit components from entering the information system.
SA-19	SA-19 (a)	CCI-003357	The organization develops anti-counterfeit policy that include the means to prevent counterfeit components from entering the information system.	The organization being inspected/assessed develops and documents an anti-counterfeit policy that include the means to prevent counterfeit components from entering the information system.	The organization conducting the inspection/assessment obtains and examines the documented anti-counterfeit policy to ensure the organization being inspected/assessed develops an anti-counterfeit policy that include the means to prevent counterfeit components from entering the information system.
SA-19	SA-19 (a)	CCI-003358	The organization develops anti-counterfeit procedures that include the means to detect counterfeit components from entering the information system.	The organization being inspected/assessed develops and documents anti-counterfeit procedures that include the means to detect counterfeit components from entering the information system.	The organization conducting the inspection/assessment obtains and examines the documented anti-counterfeit procedures to ensure the organization being inspected/assessed develops anti-counterfeit procedures that include the means to detect counterfeit components from entering the information system.
SA-19	SA-19 (a)	CCI-003359	The organization develops anti-counterfeit procedures that include the means to prevent counterfeit components from entering the information system.	The organization being inspected/assessed develops and documents anti-counterfeit procedures that include the means to prevent counterfeit components from entering the information system.	The organization conducting the inspection/assessment obtains and examines the documented anti-counterfeit procedures to ensure the organization being inspected/assessed develops anti-counterfeit procedures that include the means to prevent counterfeit components from entering the information system.
SA-19	SA-19 (a)	CCI-003360	The organization implements anti-counterfeit policy that include the means to detect counterfeit components from entering the information system.	The organization being inspected/assessed implements the policy defined in SA-19, CCIs 3356 that include the means to detect counterfeit components from entering the information system.	The organization conducting the inspection/assessment obtains and examines the policy defined in SA-19, CCIs 3356 and any artifacts applicable to counterfeit components to ensure the organization being inspected/assessed implements the policy defined in SA-19, CCIs 3356 that include the means to detect counterfeit components from entering the information system.
SA-19	SA-19 (a)	CCI-003361	The organization implements anti-counterfeit policy that include the means to prevent counterfeit components from entering the information system.	The organization being inspected/assessed implements the policy defined in SA-19, CCIs 3357 that include the means to prevent counterfeit components from entering the information system.	The organization conducting the inspection/assessment obtains and examines the policy defined in SA-19, CCIs 3357 and any artifacts applicable to counterfeit components to ensure the organization being inspected/assessed implements the policy defined in SA-19, CCIs 3357 that include the means to detect counterfeit components from entering the information system.
SA-19	SA-19 (a)	CCI-003362	The organization implements anti-counterfeit procedures that include the means to detect counterfeit components from entering the information system.	The organization being inspected/assessed implements the procedures defined in SA-19, CCIs 3358 that include the means to detect counterfeit components from entering the information system.	The organization conducting the inspection/assessment obtains and examines the procedures defined in SA-19, CCIs 3358 and any artifacts applicable to counterfeit components to ensure the organization being inspected/assessed implements the procedures defined in SA-19, CCIs 3358 that include the means to detect counterfeit components from entering the information system.
SA-19	SA-19 (a)	CCI-003363	The organization implements anti-counterfeit procedures that include the means to prevent counterfeit components from entering the information system.	The organization being inspected/assessed implements the procedures defined in SA-19, CCIs 3359 that include the means to prevent counterfeit components from entering the information system.	The organization conducting the inspection/assessment obtains and examines the procedures defined in SA-19, CCIs 3359 and any artifacts applicable to counterfeit components to ensure the organization being inspected/assessed implements the procedures defined in SA-19, CCIs 3359 that include the means to prevent counterfeit components from entering the information system.

SA-19	SA-19 (b)	CCI-003364	The organization reports counterfeit information system components to source of counterfeit component, organization-defined external reporting organizations and/or organization-defined personnel or roles.	The organization being inspected/assessed documents and implements a process to report counterfeit information system components to source of counterfeit component, at a minimum, USCYBERCOM. And/or at a minimum, the ISSO, ISSM, and PM. The organization must maintain a record of reporting. DoD has defined the personnel or roles as at a minimum, the ISSO, ISSM, and PM. DoD has defined the external reporting organizations as at a minimum, USCYBERCOM.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of reporting to ensure the organization being inspected/assessed reports counterfeit information system components to source of counterfeit component, at a minimum, USCYBERCOM. And/or at a minimum, the ISSO, ISSM, and PM.
SA-19	SA-19 (b)	CCI-003365	The organization defines the external reporting organizations to whom counterfeit information system components are to be reported.	DoD has defined the external reporting organizations as at a minimum, USCYBERCOM.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the external reporting organizations as at a minimum, USCYBERCOM
SA-19	SA-19 (b)	CCI-003366	The organization defines the personnel or roles to whom counterfeit information system components are to be reported.	DoD has defined the personnel or roles as at a minimum, the ISSO, ISSM, and PM.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as at a minimum, the ISSO, ISSM, and PM.
SC-1	SC-1 (a)	CCI-002380	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.	The organization being inspected/assessed defines and documents 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. The personnel or roles must include at a minimum, the ISSM/ISSO. DoD has defined the personnel or roles as at a minimum, the ISSO/ISSM.	The organization conducting the inspection/assessment obtains and examines the documented personnel or roles to ensure the organization being inspected/assessed 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. The personnel or roles must include at a minimum, the ISSM/ISSO. DoD has defined the personnel or roles as at a minimum, the ISSO/ISSM.
SC-1	SC-1 (a)	CCI-002378	The organization defines the personnel or roles to be recipients of the system and communications protection policy.	The organization being inspected/assessed defines and documents personnel or roles to be recipients of the system and communications protection policy. The personnel or roles must include at a minimum, the ISSM/ISSO. DoD has defined the personnel or roles as at a minimum, the ISSO/ISSM.	The organization conducting the inspection/assessment obtains and examines the documented personnel or roles to ensure the organization being inspected/assessed defines the personnel or roles to be recipients of the system and communications protection policy. The personnel or roles must include at a minimum, the ISSM/ISSO. DoD has defined the personnel or roles as at a minimum, the ISSO/ISSM.
SC-1	SC-1 (a) (1)	CCI-001074	The organization develops and documents a system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance	DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8523.01.	DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8523.01.
SC-1	SC-1 (a) (1)	CCI-001075	The organization disseminates to organization-defined personnel or roles the system and communications protection policy.	DoDI 8523.01 "Communications Security (COMSEC)"meets the DoD requirement for disseminating the system and communications protection policy. DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8523.01.	DoDI 8523.01 "Communications Security (COMSEC)"meets the DoD requirement for disseminating the system and communications protection policy. DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8523.01.
SC-1	SC-1 (a) (2)	CCI-001078	The organization develops and documents system and communications protection procedures to facilitate the implementation of the system and communications protection policy and communications protection controls and associated system and communications protection controls.	DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8523.01.	DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8523.01.
SC-1	SC-1 (a) (2)	CCI-001079	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.	DoDI 8523.01 "Communications Security (COMSEC)"meets the DoD requirement for disseminating the procedures to facilitate the implementation of the system and communications protection policy. DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8523.01.	DoDI 8523.01 "Communications Security (COMSEC)"meets the DoD requirement for disseminating the procedures to facilitate the implementation of the system and communications protection policy. DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8523.01.

SC-1	SC-1 (b) (1)	CCI-001077	The organization defines the frequency for reviewing and updating the system and communications protection policy.	DoD has defined the frequency as every 5 years.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every 5 years.
SC-1	SC-1 (b) (1)	CCI-001076	The organization reviews and updates the system and communications protection policy in accordance with organization-defined frequency.	DoDI 8523.01 "Communications Security (COMSEC)"meets the DoD requirement for reviewing and updating the system and communications protection policy. DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8523.01.	DoDI 8523.01 "Communications Security (COMSEC)"meets the DoD requirement for reviewing and updating the system and communications protection policy. DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8523.01.
SC-1	SC-1 (b) (2)	CCI-001081	The organization defines the frequency of system and communications protection procedure reviews and updates.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.
SC-1	SC-1 (b) (2)	CCI-001080	The organization reviews and updates the system and communications protection procedures in accordance with organization-defined frequency.	DoDI 8523.01 "Communications Security (COMSEC)"meets the DoD requirement for reviewing and updating the system and communications protection procedures. DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8523.01.	DoDI 8523.01 "Communications Security (COMSEC)"meets the DoD requirement for reviewing and updating the system and communications protection procedures. DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8523.01.
SC-5	SC-5	CCI-001093	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.	The organization being inspected/assessed defines and documents 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. DoD has determined the types of denial of service attacks are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented types of denial of service attacks to ensure the organization being inspected/assessed 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. DoD has determined the types of denial of service attacks are not appropriate to define at the Enterprise level.
SC-5	SC-5	CCI-002386	The organization defines the security safeguards to be employed to protect the information system against, or limit the effects of, denial of service attacks.	The organization being inspected/assessed defines and documents the security safeguards to be employed to protect the information system against, or limit the effects of, denial of service attacks. DoD has determined the security safeguards are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented security safeguards to ensure the organization being inspected/assessed defines the security safeguards to be employed to protect the information system against, or limit the effects of, denial of service attacks. DoD has determined the security safeguards are not appropriate to define at the Enterprise level.
SC-5	SC-5	CCI-002385	The information system protects against or limits the effects of organization-defined types of denial of service attacks by employing organization-defined security safeguards.	The organization being inspected/assessed configures the information system to protect against or limits the effects of types of denial of service attacks defined in SC-5, CCI 1093 by employing security safeguards defined in SC-5, CCI 2386. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2385.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to protect against or limits the effects of types of denial of service attacks defined in SC-5, CCI 1093 by employing security safeguards defined in SC-5, CCI 2386. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2385.
SC-5 (1)	SC-5 (1)	CCI-002387	The organization defines the denial of service attacks against other information systems the information system is to restrict the ability of individuals to launch.	The organization being inspected/assessed defines and documents the denial of service attacks against other information systems the information system is to restrict the ability of individuals to launch. DoD has determined the denial of service attacks as not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented denial of service attacks to ensure the organization being inspected/assessed defines the denial of service attacks against other information systems the information system is to restrict the ability of individuals to launch. DoD has determined the denial of service attacks as not appropriate to define at the Enterprise level.

SC-5 (1)	SC-5 (1)	CCI-001094	The information system restricts the ability of individuals to launch organization-defined denial of service attacks against other information systems.	The organization being inspected/assessed configures the information system to restrict the ability of individuals to launch denial of service attacks defined in SC-5 (1), CCI 2387 against other information systems. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1094.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to restrict the ability of individuals to launch denial of service attacks defined in SC-5 (1), CCI 2387 against other information systems. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1094.
SC-7	SC-7 (a)	CCI-001097	The information system monitors and controls communications at the external boundary of the system and at key internal boundaries within the system.	The organization being inspected/assessed documents and implements processes to monitor and control communications at the external boundary of the system and at key internal boundaries within the system. The organization must maintain an audit trail of monitoring activities.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of monitoring activities to ensure the organization being inspected/assessed monitors and controls communications at the external boundary of the system and at key internal boundaries within the system.
SC-7	SC-7 (b)	CCI-002395	The information system implements subnetworks for publicly accessible system components that are physically and/or logically separated from internal organizational networks.	The organization being inspected/assessed designs the information system to leverage subnetworks so that publicly accessible system components are physically and/or logically separated from internal organizational networks.	The organization conducting the inspection/assessment obtains and examines network topology diagrams, architecture documentation, or any other documentation identifying component partitioning to ensure the organization being inspected/assessed implements subnetworks for publicly accessible system components that are physically and/or logically separated from internal organizational networks.
SC-7	SC-7 (c)	CCI-001098	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.	The organization being inspected/assessed designs the information system to enforce requirements that components connect to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.	The organization conducting the inspection/assessment obtains and examines network topology diagrams, architecture documentation, or any other documentation identifying component connectivity to ensure the organization being inspected/assessed connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.
SC-7 (3)	SC-7 (3)	CCI-001101	The organization limits the number of external network connections to the information system.	The organization being inspected/assessed documents and implements information system access control mechanisms to limit the number of external connections to the information system.	The organization conducting the inspection/assessment obtains and examines the documented access control mechanisms to ensure that the organization being inspected/assessed limits the number of external network connections to the information system.
SC-7 (4)	SC-7 (4) (a)	CCI-001102	The organization implements a managed interface for each external telecommunication service.	The organization being inspected/assessed designs the information system to have a managed interface for each telecommunication service.	The organization conducting the inspection/assessment obtains and examines network topology diagrams, architecture documentation, or any other documentation identifying system interfaces to ensure the organization being inspected/assessed implements a managed interface for each external telecommunication service.
SC-7 (4)	SC-7 (4) (b)	CCI-001103	The organization establishes a traffic flow policy for each managed interface for each external telecommunication service.	The organization being inspected/assessed defines and documents a traffic flow policy for each managed interface for each external telecommunication service.	The organization conducting the inspection/assessment obtains and examines the documented traffic flow policy to ensure the organization being inspected/assessed establishes a traffic flow policy for each managed interface for each external telecommunication service.
SC-7 (4)	SC-7 (4) (c)	CCI-002396	The organization protects the confidentiality and integrity of the information being transmitted across each interface for each external telecommunication service.	The organization being inspected/assessed documents and implements mechanisms to protect the confidentiality and integrity of the information being transmitted across each interface for each external telecommunication service.	The organization conducting the inspection/assessment obtains and examines the documented mechanisms to ensure the organization being inspected/assessed protects the confidentiality and integrity of the information being transmitted across each interface for each external telecommunication service.
SC-7 (4)	SC-7 (4) (d)	CCI-001105	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.	The organization being inspected/assessed documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need for each external telecommunication service.	The organization conducting the inspection/assessment obtains and examines the documented exceptions to the traffic flow policy to ensure the organization being inspected/assessed identifies each exception with supporting mission/business need and duration of that need for each external telecommunication service.
SC-7 (4)	SC-7 (4) (e)	CCI-001107	The organization defines a frequency for the review of exceptions to the traffic flow policy for each external telecommunication service.	DoD has defined the frequency as every 180 days.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every 180 days.

SC-7 (4)	SC-7 (4) (e)	CCI-001106	The organization reviews exceptions to the traffic flow policy on an organization-defined frequency for each external telecommunication service.	The organization being inspected/assessed implements a process to review exceptions to the traffic flow policy every 180 days for each external telecommunication service. The organization must maintain an audit trail of reviews. DoD has defined the frequency as every 180 days.	The organization conducting the inspection/assessment obtains and examines the audit trail of reviews to ensure the organization being inspected/assessed reviews exceptions to the traffic flow policy every 180 days for each external telecommunication service. DoD has defined the frequency as every 180 days.
SC-7 (4)	SC-7 (4) (e)	CCI-001108	The organization removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need for each external telecommunication service.	The organization being inspected/assessed documents and implements a process to remove traffic flow policy exceptions that are no longer supported by an explicit mission/business need for each external telecommunication service.	The organization conducting the inspection/assessment obtains and examines the documented process as well as a sampling of existing exceptions to ensure the organization being inspected/assessed removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need for each external telecommunication service.
SC-7 (5)	SC-7 (5)	CCI-001109	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).	The organization being inspected/assessed configures the information system to deny network communications traffic at managed interfaces by default and allows network communications traffic by exception (i.e., deny all, permit by exception). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1109.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to deny network communications traffic at managed interfaces by default and allows network communications traffic by exception (i.e., deny all, permit by exception). For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1109.
SC-7 (7)	SC-7 (7)	CCI-002397	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.	The organization being inspected/assessed configures the information system to prevent the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2397.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to prevent the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2397.
SC-7 (8)	SC-7 (8)	CCI-001113	The organization defines the internal communications traffic to be routed to external networks.	DoD has defined the internal communications traffic as protocols as designated by PPSM guidance (e.g. HTTPS, HTTP, FTP, SNMP).	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the internal communications traffic as protocols as designated by PPSM guidance (e.g. HTTPS, HTTP, FTP, SNMP).
SC-7 (8)	SC-7 (8)	CCI-001114	The organization defines the external networks to which the organization-defined internal communications traffic should be routed.	DoD has defined the external networks as any network external to the authorization boundary.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the external networks as any network external to the authorization boundary.
SC-7 (8)	SC-7 (8)	CCI-001112	The information system routes organization-defined internal communications traffic to organization-defined external networks through authenticated proxy servers at managed interfaces.	The organization being inspected/assessed configures the information system to route protocols as designated by PPSM guidance (e.g. HTTPS, HTTP, FTP, SNMP) to any network external to the authorization boundary through authenticated proxy servers at managed interfaces. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1112. DoD has defined the internal communications traffic as protocols as designated by PPSM guidance (e.g. HTTPS, HTTP, FTP, SNMP). DoD has defined the external networks as any network external to the authorization boundary.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to route protocols as designated by PPSM guidance (e.g. HTTPS, HTTP, FTP, SNMP) to any network external to the authorization boundary through authenticated proxy servers at managed interfaces. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1112. DoD has defined the internal communications traffic as protocols as designated by PPSM guidance (e.g. HTTPS, HTTP, FTP, SNMP). DoD has defined the external networks as any network external to the authorization boundary.

SC-7 (9)	SC-7 (9) (a)	CCI-002398	The information system detects outgoing communications traffic posing a threat to external information systems.	The organization being inspected/assessed configures the information system to detect outgoing communications traffic posing a threat to external information systems. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2398.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to detect outgoing communications traffic posing a threat to external information systems. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2398.
SC-7 (9)	SC-7 (9) (a)	CCI-002399	The information system denies outgoing communications traffic posing a threat to external information systems.	The organization being inspected/assessed configures the information system to deny outgoing communications traffic posing a threat to external information systems. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2399.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to deny outgoing communications traffic posing a threat to external information systems. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2399.
SC-7 (9)	SC-7 (9) (b)	CCI-002400	The information system audits the identity of internal users associated with denied outgoing communications traffic posing a threat to external information systems.	The organization being inspected/assessed configures the information system to audit the identity of internal users associated with denied outgoing communications traffic posing a threat to external information systems. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2400.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to audit the identity of internal users associated with denied outgoing communications traffic posing a threat to external information systems. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2400.
SC-7 (10)	SC-7 (10)	CCI-001116	The organization prevents the unauthorized exfiltration of information across managed interfaces.	The organization being inspected/assessed documents and implements mechanisms to prevent the unauthorized exfiltration of information across managed interfaces.	The organization conducting the inspection/assessment obtains and examines the documented mechanisms to ensure the organization being inspected/assessed prevents the unauthorized exfiltration of information across managed interfaces.
SC-7 (11)	SC-7 (11)	CCI-002401	The organization defines the authorized sources from which the information system will allow incoming communications.	The organization being inspected/assessed defines and documents the authorized sources from which the information system will allow incoming communications. DoD has determined the authorized sources are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented authorized sources to ensure the organization being inspected/assessed defines the authorized sources from which the information system will allow incoming communications. DoD has determined the authorized sources are not appropriate to define at the Enterprise level.
SC-7 (11)	SC-7 (11)	CCI-002402	The organization defines the authorized destinations for routing inbound communications.	The organization being inspected/assessed defines and documents the authorized destinations for routing inbound communications. DoD has determined the authorized destinations are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented authorized destinations to ensure the organization being inspected/assessed defines the authorized destinations for routing inbound communications. DoD has determined the authorized destinations are not appropriate to define at the Enterprise level.
SC-7 (11)	SC-7 (11)	CCI-002403	The information system only allows incoming communications from organization-defined authorized sources routed to organization-defined authorized destinations.	The organization being inspected/assessed configures the information system to allow incoming communications from authorized sources defined in SC-7 (11), CCI 2401 routed to authorized destinations defined in SC-7 (11), CCI 2402. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2403.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to allow incoming communications from authorized sources defined in SC-7 (11), CCI 2401 routed to authorized destinations defined in SC-7 (11), CCI 2402. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2403.

SC-7 (12)	SC-7 (12)	CCI-002404	The organization defines the host-based boundary protection mechanisms that are to be implemented at organization-defined information system components.	DoD has defined the information system components as McAfee Host Intrusion Prevention (HIPS).	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the information system components as McAfee Host Intrusion Prevention (HIPS).
SC-7 (12)	SC-7 (12)	CCI-002405	The organization defines the information system components at which organization-defined host-based boundary protection mechanisms will be implemented.	DoD has defined the information system components as all information system components.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the information system components as all information system components.
SC-7 (12)	SC-7 (12)	CCI-002406	The organization implements organization-defined host-based boundary protection mechanisms at organization-defined information system components.	The organization being inspected/assessed implements McAfee Host Intrusion Prevention (HIPS) on all information system components. DoD has defined the host-based boundary protection mechanisms as McAfee Host Intrusion Prevention (HIPS). DoD has defined the information system components as all information system components.	The organization conducting the inspection/assessment examines a sampling of information system components to ensure the organization being inspected/assessed implements McAfee Host Intrusion Prevention (HIPS) on all information system components. DoD has defined the host-based boundary protection mechanisms as McAfee Host Intrusion Prevention (HIPS). DoD has defined the information system components as all information system components.
SC-7 (13)	SC-7 (13)	CCI-001120	The organization defines key information security tools, mechanisms, and support components to be isolated.	DoD has defined the key information security tools, mechanisms, and support components as key information security tools, mechanisms, and support components such as, but not limited to PKI, Patching infrastructure, HBSS, CND Tools, Special Purpose Gateway, vulnerability tracking systems, honeypots, internet access points (IAPs); network element and data center administrative/management traffic; Demilitarized Zones (DMZs), Server farms/computing centers, centralized audit log servers etc.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the key information security tools, mechanisms, and support components as key information security tools, mechanisms, and support components such as, but not limited to PKI, Patching infrastructure, HBSS, CND Tools, Special Purpose Gateway, vulnerability tracking systems, honeypots, internet access points (IAPs); network element and data center administrative/management traffic; Demilitarized Zones (DMZs), Server farms/computing centers, centralized audit log servers etc.
SC-7 (13)	SC-7 (13)	CCI-001119	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.	The organization being inspected/assessed designs the information system to isolate key information security tools, mechanisms, and support components such as, but not limited to PKI, Patching infrastructure, HBSS, CND Tools, Special Purpose Gateway, vulnerability tracking systems, honeypots, internet access points (IAPs); network element and data center administrative/management traffic; Demilitarized Zones (DMZs), Server farms/computing centers, centralized audit log servers etc. from other internal information system components by implementing physically separate subnetworks with managed interfaces to other components of the system. DoD has defined the key information security tools, mechanisms, and support components as key information security tools, mechanisms, and support components such as, but not limited to PKI, Patching infrastructure, HBSS, CND Tools, Special Purpose Gateway, vulnerability tracking systems, honeypots, internet access points (IAPs); network element and data center	The organization conducting the inspection/assessment obtains and examines network topology diagrams, architecture documentation, or any other documentation identifying component partitioning to ensure the organization being inspected/assessed isolates key information security tools, mechanisms, and support components such as, but not limited to PKI, Patching infrastructure, HBSS, CND Tools, Special Purpose Gateway, vulnerability tracking systems, honeypots, internet access points (IAPs); network element and data center administrative/management traffic; Demilitarized Zones (DMZs), Server farms/computing centers, centralized audit log servers etc. from other internal information system components by implementing physically separate subnetworks with managed interfaces to other components of the system. DoD has defined the key information security tools, mechanisms, and support components as key information security tools, mechanisms, and support components such as, but not limited to PKI, Patching infrastructure, HBSS, CND Tools, Special Purpose Gateway, vulnerability tracking systems, honeypots, internet access points (IAPs); network element and data center administrative/management traffic; Demilitarized Zones (DMZs), Server farms/computing centers, centralized audit log
SC-7 (14)	SC-7 (14)	CCI-001121	The organization protects against unauthorized physical connections at organization-defined managed interfaces.	The organization being inspected/assessed documents and implements mechanisms to protect against unauthorized physical connections at internet access points, enclave LAN to WAN, cross domain solutions, and any DoD Approved Alternate Gateways. DoD has defined the managed interfaces as internet access points, enclave LAN to WAN, cross domain solutions, and any DoD Approved Alternate Gateways.	The organization conducting the inspection/assessment obtains and examines the documented mechanisms to ensure the organization being inspected/assessed protects against unauthorized physical connections at internet access points, enclave LAN to WAN, cross domain solutions, and any DoD Approved Alternate Gateways. DoD has defined the managed interfaces as internet access points, enclave LAN to WAN, cross domain solutions, and any DoD Approved Alternate Gateways.
SC-7 (14)	SC-7 (14)	CCI-001122	The organization defines the managed interfaces where boundary protections against unauthorized physical connections are to be implemented.	DoD has defined the managed interfaces as internet access points, enclave LAN to WAN, cross domain solutions, and any DoD Approved Alternate Gateways.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the managed interfaces as internet access points, enclave LAN to WAN, cross domain solutions, and any DoD Approved Alternate Gateways.

SC-7 (14)	SC-7 (14)	CCI-002407	The organization defines the managed interfaces at which the organization protects against unauthorized physical connections.	DoD has defined the managed interfaces as internet access points, enclave LAN to WAN, cross domain solutions, and any DoD Approved Alternate Gateways.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the managed interfaces as internet access points, enclave LAN to WAN, cross domain solutions, and any DoD Approved Alternate Gateways.
SC-8	SC-8	CCI-002418	The information system protects the confidentiality and/or integrity of transmitted information.	The organization being inspected/assessed configures the information system to protect the confidentiality and/or integrity of transmitted information. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2418.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to protect the confidentiality and/or integrity of transmitted information. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2418.
SC-8 (1)	SC-8 (1)	CCI-002419	The organization defines the alternative physical safeguards to be employed when cryptographic mechanisms are not implemented to protect information during transmission.	DoD has defined the alternative physical safeguards as Protected Distribution System (PDS).	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the alternative physical safeguards as Protected Distribution System (PDS).
SC-8 (1)	SC-8 (1)	CCI-002421	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.	The organization being inspected/assessed configures the information system to implement cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission unless otherwise protected by Protected Distribution System (PDS). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2421. DoD has defined the selection as both prevention of unauthorized disclosure and detection of changes to information. DoD has defined the alternative physical safeguards as Protected Distribution System (PDS).	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission unless otherwise protected by Protected Distribution System (PDS). For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2421. DoD has defined the alternative physical safeguards as Protected Distribution System (PDS).
SC-12	SC-12	CCI-002428	The organization defines the requirements for cryptographic key generation to be employed within the information system.	DoD has defined the requirements for key generation as requirements for key generation defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the requirements for key generation as requirements for key generation defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."
SC-12	SC-12	CCI-002429	The organization defines the requirements for cryptographic key distribution to be employed within the information system.	DoD has defined the requirements for key distribution as requirements for key distribution defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the requirements for key distribution as requirements for key distribution defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."
SC-12	SC-12	CCI-002430	The organization defines the requirements for cryptographic key storage to be employed within the information system.	DoD has defined the requirements for key storage as requirements for key storage defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the requirements for key storage as requirements for key storage defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."
SC-12	SC-12	CCI-002431	The organization defines the requirements for cryptographic key access to be employed within the information system.	DoD has defined the requirements for key access as requirements for key access defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the requirements for key access as requirements for key access defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."

SC-12	SC-12	CCI-002432	The organization defines the requirements for cryptographic key destruction to be employed within the information system.	DoD has defined the requirements for key destruction as requirements for key destruction defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the requirements for key destruction as requirements for key destruction defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."
SC-12	SC-12	CCI-002433	The organization establishes cryptographic keys for required cryptography employed within the information system in accordance with organization-defined requirements for key generation.	The organization being inspected/assessed documents and implements a process to establish cryptographic keys for required cryptography employed within the information system in accordance with requirements for key generation defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key generation as requirements for key generation defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed establishes cryptographic keys for required cryptography employed within the information system in accordance with requirements for key generation defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key generation as requirements for key generation defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."
SC-12	SC-12	CCI-002434	The organization establishes cryptographic keys for required cryptography employed within the information system in accordance with organization-defined requirements for key distribution.	The organization being inspected/assessed documents and implements a process to establish cryptographic keys for required cryptography employed within the information system in accordance with requirements for key distribution defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key distribution as requirements for key distribution defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed establishes cryptographic keys for required cryptography employed within the information system in accordance with requirements for key distribution defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key distribution as requirements for key distribution defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."
SC-12	SC-12	CCI-002435	The organization establishes cryptographic keys for required cryptography employed within the information system in accordance with organization-defined requirements for key storage.	The organization being inspected/assessed documents and implements a process to establish cryptographic keys for required cryptography employed within the information system in accordance with requirements for key storage defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key storage as requirements for key storage defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed establishes cryptographic keys for required cryptography employed within the information system in accordance with requirements for key storage defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key storage as requirements for key storage defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."
SC-12	SC-12	CCI-002436	The organization establishes cryptographic keys for required cryptography employed within the information system in accordance with organization-defined requirements for key access.	The organization being inspected/assessed documents and implements a process to establish cryptographic keys for required cryptography employed within the information system in accordance with requirements for key access defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key access as requirements for key access defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed establishes cryptographic keys for required cryptography employed within the information system in accordance with requirements for key access defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key access as requirements for key access defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."

SC-12	SC-12	CCI-002437	The organization establishes cryptographic keys for required cryptography employed within the information system in accordance with organization-defined requirements for key destruction.	The organization being inspected/assessed documents and implements a process to establish cryptographic keys for required cryptography employed within the information system in accordance with requirements for key destruction defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key destruction as requirements for key destruction defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed establishes cryptographic keys for required cryptography employed within the information system in accordance with requirements for key destruction defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key destruction as requirements for key destruction defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."
SC-12	SC-12	CCI-002438	The organization manages cryptographic keys for required cryptography employed within the information system in accordance with organization-defined requirements for key generation.	The organization being inspected/assessed documents and implements a process to manage cryptographic keys for required cryptography employed within the information system in accordance with requirements for key destruction defined DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key generation as requirements for key destruction defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed manages cryptographic keys for required cryptography employed within the information system in accordance with requirements for key destruction defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key generation as requirements for key destruction defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."
SC-12	SC-12	CCI-002439	The organization manages cryptographic keys for required cryptography employed within the information system in accordance with organization-defined requirements for key distribution.	The organization being inspected/assessed documents and implements a process to manage cryptographic keys for required cryptography employed within the information system in accordance with requirements for key distribution defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key distribution as requirements for key distribution defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed manages cryptographic keys for required cryptography employed within the information system in accordance with requirements for key distribution defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key distribution as requirements for key distribution defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."
SC-12	SC-12	CCI-002440	The organization manages cryptographic keys for required cryptography employed within the information system in accordance with organization-defined requirements for key storage.	The organization being inspected/assessed documents and implements a process to manage cryptographic keys for required cryptography employed within the information system in accordance with requirements for key storage defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key storage as requirements for key storage defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed manages cryptographic keys for required cryptography employed within the information system in accordance with requirements for key storage defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key storage as requirements for key storage defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."

SC-12	SC-12	CCI-002441	The organization manages cryptographic keys for required cryptography employed within the information system in accordance with organization-defined requirements for key access.	The organization being inspected/assessed documents and implements a process to manage cryptographic keys for required cryptography employed within the information system in accordance with requirements for key access defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key access as requirements for key access defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed manages cryptographic keys for required cryptography employed within the information system in accordance with requirements for key access defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key access as requirements for key access defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."
SC-12	SC-12	CCI-002442	The organization manages cryptographic keys for required cryptography employed within the information system in accordance with organization-defined requirements for key destruction.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed manages cryptographic keys for required cryptography employed within the information system in accordance with requirements for key destruction defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key destruction as requirements for key destruction defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	The organization being inspected/assessed documents and implements a process to manage cryptographic keys for required cryptography employed within the information system in accordance with requirements for key destruction defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key destruction as requirements for key destruction defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."
SC-13	SC-13	CCI-002449	The organization defines the cryptographic uses, and type of cryptography required for each use, to be implemented by the information system.	DoD has defined the cryptographic uses and type of cryptography required for each use as protection of classified information: NSA-approved cryptography; provision of digital signatures and hashing: FIPS-validated cryptography.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the cryptographic uses and type of cryptography required for each use as protection of classified information: NSA-approved cryptography; provision of digital signatures and hashing: FIPS-validated cryptography.
SC-13	SC-13	CCI-002450	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.	The organization being inspected/assessed configures the information system to implement, for, protection of classified information: NSA-approved cryptography; for provision of digital signatures and hashing: FIPS-validated cryptography in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2450. DoD has defined the cryptographic uses and type of cryptography required for each use as protection of classified information: NSA-approved cryptography; provision of digital signatures and hashing: FIPS-validated cryptography.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement, for, protection of classified information: NSA-approved cryptography; for provision of digital signatures and hashing: FIPS-validated cryptography in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2450. DoD has defined the cryptographic uses and type of cryptography required for each use as protection of classified information: NSA-approved cryptography; provision of digital signatures and hashing: FIPS-validated cryptography.

SC-15	SC-15 (a)	CCI-001150	The information system prohibits remote activation of collaborative computing devices excluding the organization-defined exceptions where remote activation is to be allowed.	The organization being inspected/assessed configures the information system to prohibit remote activation of collaborative computing devices excluding dedicated VTC suites located in approved VTC locations that are centrally managed. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1150. DoD has defined the exceptions as dedicated VTC suites located in approved VTC locations that are centrally managed.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to prohibit remote activation of collaborative computing devices excluding dedicated VTC suites located in approved VTC locations that are centrally managed. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1150. DoD has defined the exceptions as dedicated VTC suites located in approved VTC locations that are centrally managed.
SC-15	SC-15 (a)	CCI-001151	The organization defines exceptions to the prohibiting of collaborative computing devices where remote activation is to be allowed.	DoD has defined the exceptions as dedicated VTC suites located in approved VTC locations that are centrally managed.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the exceptions as dedicated VTC suites located in approved VTC locations that are centrally managed.
SC-15	SC-15 (b)	CCI-001152	The information system provides an explicit indication of use to users physically present at collaborative computing devices.	The organization being inspected/assessed configures the information system to provide an explicit indication of use to users physically present at collaborative computing devices. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1152.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to provide an explicit indication of use to users physically present at collaborative computing devices. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1152.
SC-17	SC-17	CCI-001159	The organization issues public key certificates under an organization-defined certificate policy or obtains public key certificates from an approved service provider.	The organization being inspected/assessed configures the information system to issue public key certificates under DoDI 8520.02, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling" or obtains public key certificates from an approved service provider. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1159. DoD has defined the certificate policy as DoDI 8520.02, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling."	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to issue public key certificates under DoDI 8520.02, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling" or obtains public key certificates from an approved service provider. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1159. DoD has defined the certificate policy as DoDI 8520.02, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling."
SC-17	SC-17	CCI-002456	The organization defines the certificate policy employed to issue public key certificates.	DoD has defined the certificate policy as DoDI 8520.02, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling."	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the certificate policy as DoDI 8520.02, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling.
SC-18	SC-18 (a)	CCI-001160	The organization defines acceptable and unacceptable mobile code and mobile code technologies.	The organization being inspected/assessed defines and documents acceptable and unacceptable mobile code and mobile code technologies IAW the Protection Profile for Web Browsers and Application SRG. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must define IAW the STIG/SRG guidance that pertains to CCI 1160.	The organization conducting the inspection/assessmenet obtains and examines the documented acceptable and unacceptable mobile code and mobile code technologies to ensure the organization being inspected/assessed defines acceptable and unacceptable mobile code and mobile code technologies IAW the Protection Profile for Web Browsers and Application SRG. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has defined acceptable and unacceptable mobile code and mobile code technologies IAW the applicable STIGs and SRGs pertaining to CCI 1160.

SC-18	SC-18 (b)	CCI-001161	The organization establishes usage restrictions for acceptable mobile code and mobile code technologies.	The organization being inspected/assessed documents usage restrictions for acceptable mobile code and mobile code technologies IAW the Protection Profile for Web Browsers and Application SRG. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must establish IAW the STIG/SRG guidance that pertains to CCI 1161.	The organization conducting the inspection/assessmenet obtains and examines the documented usage restrictions to ensure the organization being inspected/assessed establishes usage restrictions for acceptable mobile code and mobile code technologies IAW the Protection Profile for Web Browsers and Application SRG. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has established usage restrictions IAW the applicable STIGs and SRGs pertaining to CCI 1161.
SC-18	SC-18 (b)	CCI-001162	The organization establishes implementation guidance for acceptable mobile code and mobile code technologies.	The Protection Profile for Web Browsers and Application SRG meet the DoD requirement to establishe implementation guidance for acceptable mobile code and mobile code technologies. DoD Components are automatically compliant with this control because they are covered by the Protection Profile for Web Browsers and Application SRG.	The Protection Profile for Web Browsers and Application SRG meet the DoD requirement to establishe implementation guidance for acceptable mobile code and mobile code technologies. DoD Components are automatically compliant with this control because they are covered by the Protection Profile for Web Browsers and Application SRG.
SC-18	SC-18 (c)	CCI-001163	The organizations authorizes the use of mobile code within the information system.	The organization being inspected/assessed documents mobile code which is authorized for use within the information system.	The organization conducting the inspection/assessment obtains and examines the documented list of mobile code which is authorized for use within the information system and examines the information system to ensure that all used mobile code is authorized.
SC-18	SC-18 (c)	CCI-001164	The organization monitors the use of mobile code within the information system.	The organization being inspected/assessed documents and implements a process to monitor the use of mobile code within the information system.	The organization conducting the inspection/assessment obtains and examines the documented process as well as any artifacts applicable to monitoring of mobile code to ensure the organization being inspected/assessed monitors the use of mobile code within the information system.
SC-18	SC-18 (c)	CCI-001165	The organization controls the use of mobile code within the information system.	The organization being inspected/assessed documents and implements a process to control the use of mobile code within the information system.	The organization conducting the inspection/assessment obtains and examines the documented process and examines the information system to ensure the organization being inspected/assessed controls the use of mobile code within the information system.
SC-18 (1)	SC-18 (1)	CCI-001166	The information system identifies organization-defined unacceptable mobile code.	The organization being inspected/assessed configures the information system to identify unacceptable mobile code defined in SC-18 (1), CCI 2458. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1166.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to identify unacceptable mobile code defined in SC-18 (1), CCI 2458. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1166.
SC-18 (1)	SC-18 (1)	CCI-001662	The information system takes organization-defined corrective action when organization-defined unacceptable mobile code is identified.	The organization being inspected/assessed configures the information system to take corrective actions defined in SC-18 (1), CCI 2457 when unacceptable mobile code defined in SC-18 (1), CCI 2458 is identified. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1662.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to take corrective actions defined in SC-18 (1), CCI 2457 when unacceptable mobile code defined in SC-18 (1), CCI 2458 is identified. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1662.
SC-18 (1)	SC-18 (1)	CCI-002457	The organization defines the corrective actions to be taken when organization-defined unacceptable mobile code is identified.	DoD has defined the corrective actions to be taken when organization-defined unacceptable mobile code is identified as the corrective actions defined in the Protection Profile for Web Browsers and Application SRG.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the corrective actions to be taken when organization-defined unacceptable mobile code is identified as the corrective actions defined in the Protection Profile for Web Browsers and Application SRG.

SC-18 (1)	SC-18 (1)	CCI-002458	The organization defines what constitutes unacceptable mobile code for its information systems.	The organization being inspected/assessed defines and documents unacceptable mobile code IAW the Protection Profile for Web Browsers and Application SRG. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must define IAW the STIG/SRG guidance that pertains to CCI 2458. DoD has determined the unnacceptable mobile code is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessmenet obtains and examines the documented acceptable and unacceptable mobile code and mobile code technologies to ensure the organization being inspected/assessed defines unacceptable mobile code IAW the Protection Profile for Web Browsers and Application SRG. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has defined unacceptable mobile code IAW the applicable STIGs and SRGs pertaining to CCI 2458. DoD has determined the unnacceptable mobile code is not appropriate to define at the Enterprise level.
SC-18 (2)	SC-18 (2)	CCI-001167	The organization ensures the development of mobile code to be deployed in information systems meets organization-defined mobile code requirements.	The organization being inspected/assessed documents and implements a process to develop mobile code IAW the requirements defined in CCI 1168.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed develops mobile code IAW the requirements defined in CCI 1168.
SC-18 (2)	SC-18 (2)	CCI-001168	The organization defines requirements for the acquisition, development, and use of mobile code.	The organization being inspected/assessed defines and documents requirements for the acquisition, development, and use of mobile code. The requirements must result in the acquisition and development of mobile code which complies with the Protection Profile for Web Browsers and Application SRG. DoD has determined the requirements are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented requirements to ensure the organization being inspected/assessed defines requirements for the acquisition, development, and use of mobile code. DoD has determined the requirements are not appropriate to define at the Enterprise level.
SC-18 (2)	SC-18 (2)	CCI-001687	The organization ensures the use of mobile code to be deployed in information systems meets organization-defined mobile code requirements.	The organization being inspected/assessed documents and implements a process to use mobile code IAW the requirements defined in CCI 1168.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed uses mobile code IAW the requirements defined in CCI 1168.
SC-18 (2)	SC-18 (2)	CCI-001688	The organization ensures the acquisition of mobile code to be deployed in information systems meets organization-defined mobile code requirements.	The organization being inspected/assessed documents and implements a process to acquire mobile code IAW the requirements defined in CCI 1168.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed acquire mobile code IAW the requirements defined in CCI 1168.
SC-18 (3)	SC-18 (3)	CCI-002459	The organization defines the unacceptable mobile code of which the information system is to prevent download and execution.	The organization being inspected/assessed defines and documents unacceptable mobile code of which the information system is to prevent download and execution IAW the Protection Profile for Web Browsers and Application SRG. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must define IAW the STIG/SRG guidance that pertains to CCI 2459. DoD has determined the unnaceptable mobile code is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessmenet obtains and examines the documented unacceptable mobile code to ensure the organization being inspected/assessed defines unacceptable mobile code of which the information system is to prevent download and execution IAW the Protection Profile for Web Browsers and Application SRG. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has defined unacceptable mobile code IAW the applicable STIGs and SRGs pertaining to CCI 2459. DoD has determined the unnaceptable mobile code is not appropriate to define at the Enterprise level.
SC-18 (3)	SC-18 (3)	CCI-001169	The information system prevents the download of organization-defined unacceptable mobile code.	The organization being inspected/assessed configures the information system to prevent the download of unacceptable mobile code defined in CCI 2459. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1169.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to prevent the download of unacceptable mobile code defined in CCI 2459. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1169.

SC-18 (3)	SC-18 (3)	CCI-001695	The information system prevents the execution of organization-defined unacceptable mobile code.	The organization being inspected/assessed configures the information system to prevent the execution of unacceptable mobile code defined in CCI 2459. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1695.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to prevent the execution of unacceptable mobile code defined in CCI 2459. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1695.
SC-18 (4)	SC-18 (4)	CCI-001171	The organization defines software applications in which automatic mobile code execution is to be prohibited	DoD has defined the software applications in which automatic mobile code execution is to be prohibited as the software applications defined in the Protection Profile for Web Browsers and Application SRG.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the software applications in which automatic mobile code execution is to be prohibited as the software applications defined in the Protection Profile for Web Browsers and Application SRG.
SC-18 (4)	SC-18 (4)	CCI-001170	The information system prevents the automatic execution of mobile code in organization-defined software applications.	The organization being inspected/assessed configures the information system to prevent the automatic execution of unacceptable mobile code in software applications defined in CCI 1171. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1170.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to prevent the automatic execution of unacceptable mobile code in software applications defined in CCI 1171. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1170.
SC-18 (4)	SC-18 (4)	CCI-001172	The organization defines actions to be enforced by the information system before executing mobile code.	DoD has defined the actions as the user be prompted.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the actions as the user be prompted.
SC-18 (4)	SC-18 (4)	CCI-002460	The information system enforces organization-defined actions prior to executing the code.	The organization being inspected/assessed configures the information system to prompt the user prior to executing the code. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2460. DoD has defined the actions as the user be prompted.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to prompt the user prior to executing the code. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2460. DoD has defined the actions as the user be prompted.
SC-19	SC-19 (a)	CCI-001173	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.	The organization being inspected/assessed establishes and documents usage restrictions for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously.	The organization conducting the inspection/assessment obtains and examines the documented usage restrictions to ensure the organization being inspected/assessed establishes usage restrictions for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously.
SC-19	SC-19 (a)	CCI-001174	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.	The Voice and Video over Internet Protocol (V-VoIP) STIG meets the DoD requirement for establishing implementation guidance for Voice over Internet Protocol (VoIP) technologies. DoD Components are automatically compliant with this control because they are covered by the DoD level policy, V-VoIP STIG.	The V-VoIP STIG meets the DoD requirement for establishing implementation guidance for Voice over Internet Protocol (VoIP) technologies. DoD Components are automatically compliant with this control because they are covered by the DoD level policy, V-VoIP STIG.
SC-19	SC-19 (b)	CCI-001175	The organization authorizes the use of VoIP within the information system.	The organization being inspected/assessed authorizes any appropriate usage of VoIP within the information system and documents those authorizations.	The organization conducting the inspection/assessment obtains and examines the documented authorizations and *insert language* to ensure the organization being inspected/assessed authorizes any appropriate usage of VoIP within the information system and documents those authorizations.

SC-19	SC-19 (b)	CCI-001176	The organization monitors the use of VoIP within the information system.	The organization being inspected/assessed documents and implements a process to monitor the use of VoIP within the information system. The organization must maintain an audit trail of monitoring.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trial of monitoring to ensure the organization being inspected/assessed monitors the use of VoIP within the information system.
SC-19	SC-19 (b)	CCI-001177	The organization controls the use of VoIP within the information system.	The organization being inspected/assessed designs the information system to control the use of VoIP within the information system	The organization conducting the inspection/assessment obtains and examines network topology diagrams, architecture documentation, or any other documentation identifying the use of VoIP to ensure the organization being inspected/assessed controls the use of VoIP within the information system.
SC-20	SC-20 (a)	CCI-001178	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.	The organization being inspected/assessed configures the authoritative name server software for external queries to enable DNSSEC and creates resource records with digital signatures (RRSig) for each A record. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that determines the name server software configuration files and pertains to CCI 1178.	The organization conducting the inspection/assessment: 1. inspects the configuration files for the presence of DNSSEC records for each A record hosted in a zone; 2. utilizes DNSSEC diagnostic tools, such as dig; and 3. performs queries which will exercise the data flow path for authoritative name resolution services. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs that determine the name server software configuration files and pertain to CCI 1178.
SC-20	SC-20 (a)	CCI-002462	The information system provides additional integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries.	The organization being inspected/assessed configures the authoritative name server software for external queries to enable DNSSEC and creates resource records with digital signatures (RRSig) for each A record. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that determines the name server software configuration files and pertains to CCI 2462.	The organization conducting the inspection/assessment: 1. inspects the configuration files for the presence of DNSSEC records for each A record hosted in a zone; 2. utilizes DNSSEC diagnostic tools, such as dig; and 3. performs queries which will exercise the data flow path for authoritative name resolution services. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs that determine the name server software configuration files and pertain to CCI 2462.
SC-20	SC-20 (b)	CCI-001179	The information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child zones.	The organization being inspected/assessed configures the authoritative name server software to enable DNSSEC and creates delegation signer (DS) resource records for each child zone and place those records in the parent zone. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that determines the name server software configuration files and pertains to CCI 1179.	The organization conducting the inspection/assessment inspect the configuration files for the presence of Delegation Signer (DS) Records for any child domains. Note: This is only applicable for zones with child domains. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs that determine the name server software configuration files and pertain to CCI 1179.
SC-20	SC-20 (b)	CCI-001663	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).	The organization being inspected/assessed installs and utilizes software capable of validating the chain of trust (Examples of software include dig, dnsviz, dnssec-debugger, dnssec validator for Mozilla, etc.). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1663.	The organization conducting the inspection/assessment utilizes DNSSEC diagnostic tools, such as dig, and performs queries which will exercise the data flow path for authoritative name resolution services where parent and child domains exist. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs that pertains to CCI 1663.

SC-21	SC-21	CCI-002465	The information system requests data origin authentication verification on the name/address resolution responses the system receives from authoritative sources.	The organization being inspected/assessed configures the: 1. recursive/caching name server software to enable DNSSEC; 2. software to enable DNSSEC validation; and 3. software to establish a secure entry point trust anchor by installing key signing keys in the software configuration of trusted keys. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that determines the name server software configuration files and pertains to CCI 2465.	The organization conducting the inspection/assessment utilizes DNSSEC diagnostic tools, such as dig, and performs queries which will exercise the data flow path for recursive name resolution services. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs that determine the name server software configuration files and pertain to CCI 2465.
SC-21	SC-21	CCI-002466	The information system requests data integrity verification on the name/address resolution responses the system receives from authoritative sources.	The organization being inspected/assessed configures the: 1. recursive/caching name server software to enable DNSSEC; 2. software to enable DNSSEC validation; and 3. software to establish a secure entry point trust anchor by installing key signing keys in the software configuration of trusted keys. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that determines the name server software configuration files and pertains to CCI 2466.	The organization conducting the inspection/assessment utilizes DNSSEC diagnostic tools, such as dig, and performs queries which will exercise the data flow path for recursive name resolution services. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs that determine the name server software configuration files and pertain to CCI 2466.
SC-21	SC-21	CCI-002467	The information system performs data integrity verification on the name/address resolution responses the system receives from authoritative sources.	The organization being inspected/assessed configures the: 1. recursive/caching name server software to enable DNSSEC; 2. software to enable DNSSEC validation; and 3. software to establish a secure entry point trust anchor by installing key signing keys in the software configuration of trusted keys. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that determines the name server software configuration files and pertains to CCI 2467.	The organization conducting the inspection/assessment utilizes DNSSEC diagnostic tools, such as dig, and performs queries which will exercise the data flow path for recursive name resolution services. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs that determine the name server software configuration files and pertain to CCI 2467.
SC-21	SC-21	CCI-002468	The information system performs data origin verification authentication on the name/address resolution responses the system receives from authoritative sources.	The organization being inspected/assessed configures the: 1. recursive/caching name server software to enable DNSSEC; 2. software to enable DNSSEC validation; and 3. software to establish a secure entry point trust anchor by installing key signing keys in the software configuration of trusted keys. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that determines the name server software configuration files and pertains to CCI 2468.	The organization conducting the inspection/assessment utilizes DNSSEC diagnostic tools, such as dig, and performs queries which will exercise the data flow path for recursive name resolution services. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs that determine the name server software configuration files and pertain to CCI 2468.
SC-22	SC-22	CCI-001182	The information systems that collectively provide name/address resolution service for an organization are fault-tolerant.	The organization being inspected/assessed implements a name service resolution architecture consisting of primary and secondary servers. The organization must document the architecture in the site security plan. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1182.	The organization conducting the inspection/assessment reviews the sites implementation documentation of the name resolution servers and verifies primary and alternate services are available. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1182.

SC-22	SC-22	CCI-001183	The information systems that collectively provide name/address resolution service for an organization implement internal/external role separation.	The organization being inspected/assessed implements a name service resolution architecture where recursive and authoritative server software is not installed on the same information system. The organization must document the architecture in the site security plan. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1183.	The organization conducting the inspection/assessment reviews the sites implementation documentation of the name resolution servers and verifies authoritative and recursive services are not hosted on the same information system. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1183.
SC-23	SC-23	CCI-001184	The information system protects the authenticity of communications sessions.	The organization being inspected/assessed configures the information system to protect the authenticity of communications sessions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1184.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to protect the authenticity of communications sessions. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1184.
SC-23 (1)	SC-23 (1)	CCI-001185	The information system invalidates session identifiers upon user logout or other session termination.	The organization being inspected/assessed configures the information system to invalidate session identifiers upon user logout or other session termination. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1185.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to invalidate session identifiers upon user logout or other session termination. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1185.
SC-23 (3)	SC-23 (3)	CCI-001188	The information system generates unique session identifiers for each session with organization-defined randomness requirements.	The organization being inspected/assessed configures the information system to generate unique session identifiers for each session with randomness requirements defined in SC-23 (3), CCI 1189. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1188.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to generate unique session identifiers for each session with randomness requirements defined in SC-23 (3), CCI 1189. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1188.
SC-23 (3)	SC-23 (3)	CCI-001189	The organization defines randomness requirements for generating unique session identifiers.	The organization being inspected/assessed defines and documents randomness requirements for generating unique session identifiers. DoD has determined the randomness requirements are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented randomness requirements to ensure the organization being inspected/assessed defines randomness requirements for generating unique session identifiers. DoD has determined the randomness requirements are not appropriate to define at the Enterprise level.
SC-23 (3)	SC-23 (3)	CCI-001664	The information system recognizes only session identifiers that are system-generated.	The organization being inspected/assessed configures the information system to recognize only session identifiers that are system-generated. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1664.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to recognize only session identifiers that are system-generated. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1664.
SC-23 (5)	SC-23 (5)	CCI-002469	The organization defines the certificate authorities the information system will allow to be used on the information system.	DoD has defined the certificate authorities as DoD PKI established certificate authorities.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the certificate authorities as DoD PKI established certificate authorities.

SC-23 (5)	SC-23 (5)	CCI-002470	The information system only allows the use of organization-defined certificate authorities for verification of the establishment of protected sessions.	The organization being inspected/assessed configures the information system to allow the use of DoD PKI established certificate authorities for verification of the establishment of protected sessions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2470. DoD has defined the certificate authorities as DoD PKI established certificate authorities.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to allow the use of DoD PKI established certificate authorities for verification of the establishment of protected sessions. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2470. DoD has defined the certificate authorities as DoD PKI established certificate authorities.
SC-28	SC-28	CCI-001199	The information system protects the confidentiality and/or integrity of organization-defined information at rest.	The organization being inspected/assessed configures the information system to protect the confidentiality and/or integrity of organization-defined information at rest. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1199.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to protect the confidentiality and/or integrity of organization-defined information at rest. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1199.
SC-28	SC-28	CCI-002472	The organization defines the information at rest that is to be protected by the information system.	The organization being inspected/assessed defines and documents the information at rest that is to be protected by the information system which must include, at a minimum, PII and classified information. DoD has determined the information at rest is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented information at rest to ensure the organization being inspected/assessed defines and documents the information at rest that is to be protected by the information system which must include, at a minimum, PII and classified information. DoD has determined the information at rest is not appropriate to define at the Enterprise level.
SC-28 (1)	SC-28 (1)	CCI-002473	The organization defines the information at rest for which cryptographic mechanisms will be implemented.	The organization being inspected/assessed defines and documents the information at rest that is to be protected by the information system which must include, at a minimum, PII and classified information. DoD has determined the information at rest is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented information at rest to ensure the organization being inspected/assessed defines and documents the information at rest that is to be protected by the information system which must include, at a minimum, PII and classified information. DoD has determined the information at rest is not appropriate to define at the Enterprise level.
SC-28 (1)	SC-28 (1)	CCI-002474	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.	DoD has defined the information system components as any information system components storing data defined in SC-28 (1), 2473.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the information system components as any information system components storing data defined in SC-28 (1), 2473.
SC-28 (1)	SC-28 (1)	CCI-002475	The information system implements cryptographic mechanisms to prevent unauthorized modification of organization-defined information at rest on organization-defined information system components.	The organization being inspected/assessed configures the information system to implement cryptographic mechanisms to prevent unauthorized modification of information at rest defined in SC-28 (1), CCI 2473 on any information system components storing data defined in SC-28 (1), 2473. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2475. DoD has defined the information system components as any information system components storing data defined in SC-28 (1), 2473.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement cryptographic mechanisms to prevent unauthorized modification of information at rest defined in SC-28 (1), CCI 2473 on any information system components storing data defined in SC-28 (1), 2473. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2475. DoD has defined the information system components as any information system components storing data defined in SC-28 (1), 2473.

SC-28 (1)	SC-28 (1)	CCI-002476	The information system implements cryptographic mechanisms to prevent unauthorized disclosure of organization-defined information at rest on organization-defined information system components.	The organization being inspected/assessed configures the information system to implement cryptographic mechanisms to prevent unauthorized disclosure of information at rest defined in SC-28 (1), CCI 2473 on any information system components storing data defined in SC-28 (1), 2473. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2476. DoD has defined the information system components as any information system components storing data defined in SC-28 (1), 2473.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement cryptographic mechanisms to prevent unauthorized disclosure of information at rest defined in SC-28 (1), CCI 2473 on any information system components storing data defined in SC-28 (1), 2473. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2476. DoD has defined the information system components as any information system components storing data defined in SC-28 (1), 2473.
SC-38	SC-38	CCI-002528	The organization defines the operations security safeguards to be employed to protect key organizational information throughout the system development life cycle.	The organization being inspected/assessed defines and documents the operations security safeguards to be employed to protect key organizational information throughout the system development life cycle. DoD has determined the operations security safeguards are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented operations security safeguards to ensure the organization being inspected/assessed defines the operations security safeguards to be employed to protect key organizational information throughout the system development life cycle. DoD has determined the operations security safeguards are not appropriate to define at the Enterprise level.
SC-38	SC-38	CCI-002529	The organization employs organization-defined operations security safeguards to protect key organizational information throughout the system development life cycle.	The organization being inspected/assessed implements operations security safeguards defined in SC-38, CCI 2528 to protect key organizational information throughout the system development life cycle. The organization must maintain an audit trail of security safeguard implementation.	The organization conducting the inspection/assessment obtains and examines the audit trail of security safeguard implementation to ensure the organization being inspected/assessed employs operations security safeguards defined in SC-38, CCI 2528 to protect key organizational information throughout the system development life cycle.
SC-39	SC-39	CCI-002530	The information system maintains a separate execution domain for each executing process.	The organization being inspected/assessed configures the information system to maintain a separate execution domain for each executing process. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2530.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to maintain a separate execution domain for each executing process. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2530.
SI-1	SI-1 (a)	CCI-002601	The organization defines the personnel or roles to whom the system and information integrity policy and procedures are to be disseminated.	DoD has defined the roles as all appointed information assurance personnel.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the roles as all appointed information assurance personnel.
SI-1	SI-1 (a) (1)	CCI-001217	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.	Documenting and implementing the Risk Management Framework (RMF) for DoD IT (DoDI 8510.01) meets the DoD requirement for a system and information integrity policy. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, Risk Management Framework (RMF) for DoD IT (DoDI 8510.01).	Documenting and implementing the Risk Management Framework (RMF) for DoD IT (DoDI 8510.01) meets the DoD requirement for a system and information integrity policy. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, Risk Management Framework (RMF) for DoD IT (DoDI 8510.01).
SI-1	SI-1 (a) (1)	CCI-001218	The organization disseminates the system and information integrity policy to organization-defined personnel or roles.	DoD disseminates DoDI 8510.01 via the DoD Issuances website (http://www.dtic.mil/whs/directives/corres/dir.html) that meets the DoD requirement for a system and information integrity policy. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, Risk Management Framework (RMF) for DoD IT (DoDI 8510.01).	Documenting and implementing the Risk Management Framework (RMF) for DoD IT (DoDI 8510.01) meets the DoD requirement for a system and information integrity policy. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, Risk Management Framework (RMF) for DoD IT (DoDI 8510.01).

SI-1	SI-1 (a) (2)	CCI-001220	The organization develops and documents procedures to facilitate the implementation of the system and information integrity policy and associated system integrity controls.	Documenting and implementing the Risk Management Framework (RMF) for DoD IT (DoDI 8510.01) meets the DoD requirement for a system and information integrity policy. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, Risk Management Framework (RMF) for DoD IT (DoDI 8510.01).	Documenting and implementing the Risk Management Framework (RMF) for DoD IT (DoDI 8510.01) meets the DoD requirement for a system and information integrity policy. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, Risk Management Framework (RMF) for DoD IT (DoDI 8510.01).
SI-1	SI-1 (a) (2)	CCI-001221	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.	DoD disseminates DoDI 8510.01 via the DoD Issuances website (http://www.dtic.mil/whs/directives/corres/dir.html) that meets the DoD requirement for a system and information integrity policy. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, Risk Management Framework (RMF) for DoD IT (DoDI 8510.01).	Documenting and implementing the Risk Management Framework (RMF) for DoD IT (DoDI 8510.01) meets the DoD requirement for a system and information integrity policy. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, Risk Management Framework (RMF) for DoD IT (DoDI 8510.01).
SI-1	SI-1 (b) (1)	CCI-001223	The organization defines the frequency of system and information integrity policy reviews and updates.	DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10.
SI-1	SI-1 (b) (1)	CCI-001219	The organization reviews and updates system and information integrity policy in accordance with organization-defined frequency.	Documenting and implementing the Risk Management Framework (RMF) for DoD IT (DoDI 8510.01) meets the DoD requirement for a system and information integrity policy. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, Risk Management Framework (RMF) for DoD IT (DoDI 8510.01).	Documenting and implementing the Risk Management Framework (RMF) for DoD IT (DoDI 8510.01) meets the DoD requirement for a system and information integrity policy. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, Risk Management Framework (RMF) for DoD IT (DoDI 8510.01).
SI-1	SI-1 (b) (2)	CCI-001224	The organization defines the frequency of system and information integrity procedure reviews and updates	DoD has defined the frequency as reviewed annually - updated as appropriate.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as reviewed annually - updated as appropriate.
SI-1	SI-1 (b) (2)	CCI-001222	The organization reviews and updates system and information integrity procedures in accordance with organization-defined frequency.	Documenting and implementing the Risk Management Framework (RMF) for DoD IT (DoDI 8510.01) meets the DoD requirement for a system and information integrity policy. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, Risk Management Framework (RMF) for DoD IT (DoDI 8510.01).	Documenting and implementing the Risk Management Framework (RMF) for DoD IT (DoDI 8510.01) meets the DoD requirement for a system and information integrity policy. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, Risk Management Framework (RMF) for DoD IT (DoDI 8510.01).
SI-2	SI-2 (a)	CCI-001225	The organization identifies information system flaws.	The organization being inspected/assessed documents and implements a process to identify information system flaws. The process shall include review of the system through automated scans and manual checks to determine the existence of flaws such as IAVM, CVE, or other resources.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed identifies information system flaws.
SI-2	SI-2 (a)	CCI-001226	The organization reports information system flaws.	The organization being inspected/assessed reports information system flaws according to DoD Cybersecurity policy and organizational roles and responsibilities. The organization must report information system flaws in their POA&M.	The organization conducting the inspection/assessment obtains and examines the authorization package, verifies the POA&M is up to date and includes recently identified information system flaws, and verifies that the organization has notified appropriate personnel as defined by DoD Cybersecurity policy and organizational roles and responsibilities.
SI-2	SI-2 (a)	CCI-001227	The organization corrects information system flaws.	The organization being inspected/assessed corrects information system flaws within the time period directed by an authorative source (e.g. IAVM, CTOs, DTMs, STIGs). The organization documents the corrections on their POA&M. DoD has defined the time period as within the time period directed by an authorative source (e.g. IAVM, CTOs, DTMs, STIGs).	The organization conducting the inspection/assessment obtains and examines the information system POA&M and examines the information system to ensure the organization being inspected/assessed corrects information system flaws.

SI-2	SI-2 (b)	CCI-001228	The organization tests software updates related to flaw remediation for effectiveness before installation.	The organization being inspected/assessed documents and implements a process to test software updates related to flaw remediation for effectiveness before installation. If the software update is being provided by a vendor who has documented the effectiveness of the update in fixing the affected IAVM/CVE, further testing by the organization may not be required.	The organization conducting the inspection/assessment obtains and examines the documented process and test results to ensure the organization being inspected/assessed tests software updates related to flaw remediation for effectiveness before installation.
SI-2	SI-2 (b)	CCI-001229	The organization tests software updates related to flaw remediation for potential side effects before installation.	The organization being inspected/assessed documents and implements a process for regression testing IAW CM-4 to identify any potential side effects before installation of software updates.	The organization conducting the inspection/assessment obtains and examines the documented process and test results to ensure the organization being inspected/assessed tests software updates related to flaw remediation for potential side effects before installation.
SI-2	SI-2 (d)	CCI-001230	The organization incorporates flaw remediation into the organizational configuration management process.	The organization being inspected/assessed documents within their configuration management plan, flaw remediation processes.	The organization conducting the inspection/assessment obtains and examines the configuration management plan to ensure that it incorporates flaw remediation.
SI-2	SI-2 (b)	CCI-002602	The organization tests firmware updates related to flaw remediation for effectiveness before installation.	The organization being inspected/assessed documents and implements a process to test firmware updates related to flaw remediation for effectiveness before installation. If the firmware update is being provided by a vendor who has documented the effectiveness of the update in fixing the affected IAVM/CVE, further testing by the organization may not be required.	The organization conducting the inspection/assessment obtains and examines the documented process and test results to ensure the organization being inspected/assessed tests firmware updates related to flaw remediation for effectiveness before installation.
SI-2	SI-2 (b)	CCI-002603	The organization tests firmware updates related to flaw remediation for potential side effects before installation.	The organization being inspected/assessed documents and implements a process for regression testing IAW CM-4 to identify any potential side effects before installation of software updates.	The organization conducting the inspection/assessment obtains and examines the documented process and test results to ensure the organization being inspected/assessed tests firmware updates related to flaw remediation for potential side effects before installation.
SI-2	SI-2 (c)	CCI-002604	The organization defines the time period within the release of updates that security-related software updates are to be installed.	DoD has defined the time period as 30 days.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as 30 days
SI-2	SI-2 (c)	CCI-002605	The organization installs security-relevant software updates within organization-defined time period of the release of the updates	The organization being inspected/assessed configures the information system to install security-relevant software updates within 30 days of the release of the updates For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2605. DoD has defined the time period as 30 days.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to install security-relevant software updates within 30 days of the release of the updates. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2605. DoD has defined the time period as 30 days.
SI-2	SI-2 (c)	CCI-002606	The organization defines the time period within the release of updates that security-related firmware updates are to be installed.	DoD has defined the time period as 30 days.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as 30 days
SI-2	SI-2 (c)	CCI-002607	The organization installs security-relevant firmware updates within organization-defined time period of the release of the updates	The organization being inspected/assessed configures the information system to install security-relevant firmware updates within 30 days of the release of the updates. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2607. DoD has defined the time period as 30 days.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to install security-relevant firmware updates within 30 days of the release of the updates. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2607. DoD has defined the time period as 30 days.
SI-2 (1)	SI-2 (1)	CCI-001231	The organization centrally manages the flaw remediation process.	The organization being inspected/assessed documents and implements a process to centrally manage the flaw remediation process.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed centrally manages the flaw remediation process.

SI-2 (2)	SI-2 (2)	CCI-001234	The organization defines a frequency for employing automated mechanisms to determine the state of information system components with regard to flaw remediation.	DoD has defined the frequency as continuously with HBSS; 30 days for any additional internal network scans not covered by HBSS; annually for external scans by (Computer Network Defense Service Provider) CNDSP.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as continuously with HBSS; 30 days for any additional internal network scans not covered by HBSS; annually for external scans by (Computer Network Defense Service Provider) CNDSP.
SI-2 (2)	SI-2 (2)	CCI-001233	The organization employs automated mechanisms on an organization-defined frequency to determine the state of information system components with regard to flaw remediation.	The organization being inspected/assessed configures the information system to employ automated mechanisms continuously with HBSS; 30 days for any additional internal network scans not covered by HBSS; annually for external scans by (Computer Network Defense Service Provider) CNDSP to determine the state of information system components with regard to flaw remediation. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1233. DoD has defined the frequency as continuously with HBSS; 30 days for any additional internal network scans not covered by HBSS; annually for external scans by (Computer Network Defense Service Provider) CNDSP.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to employ automated mechanisms continuously with HBSS; 30 days for any additional internal network scans not covered by HBSS; annually for external scans by (Computer Network Defense Service Provider) CNDSP to determine the state of information system components with regard to flaw remediation. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1233. DoD has defined the frequency as continuously with HBSS; 30 days for any additional internal network scans not covered by HBSS; annually for external scans by (Computer Network Defense Service Provider) CNDSP.
SI-2 (3)	SI-2 (3) (a)	CCI-001235	The organization measures the time between flaw identification and flaw remediation.	The organization being inspected/assessed documents and implements a process to measure the time between flaw identification and flaw remediation. The organization must maintain an audit trail of flaw identification and flaw remediation.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of flaw identification and flaw remediation to ensure the organization being inspected/assessed measures the time between flaw identification and flaw remediation.
SI-2 (3)	SI-2 (3) (b)	CCI-001236	The organization defines benchmarks for the time taken to apply corrective actions after flaw identification.	DoD has defined the benchmarks as within the time period directed by an authorative source (e.g. IAVM, CTOs, DTMs, STIGs).	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the benchmarks as within the time period directed by an authorative source (e.g. IAVM, CTOs, DTMs, STIGs).
SI-2 (3)	SI-2 (3) (b)	CCI-002608	The organization establishes organization-defined benchmarks for the time taken to apply corrective actions after flaw identification.	The organization being inspected/assessed implements benchmarks for the time taken to apply corrective actions after flaw identification IAW the period directed by an authorative source (e.g. IAVM, CTOs, DTMs, STIGs). DoD has defined the benchmarks as within the time period directed by an authorative source (e.g. IAVM, CTOs, DTMs, STIGs).	The organization conducting the inspection/assessment obtains and examines records of corrective actions taken to ensure the organization being inspected/assessed implements benchmarks for the time taken to apply corrective actions after flaw identification IAW the period directed by an authorative source (e.g. IAVM, CTOs, DTMs, STIGs). DoD has defined the benchmarks as within the time period directed by an authorative source (e.g. IAVM, CTOs, DTMs, STIGs).
SI-2 (6)	SI-2 (6)	CCI-002615	The organization defines the software components to be removed (e.g., previous versions) after updated versions have been installed.	DoD has defined the software components as all upgraded/replaced software components that are no longer required for operation.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the software components as all upgraded/replaced software components that are no longer required for operation.
SI-2 (6)	SI-2 (6)	CCI-002616	The organization defines the firmware components to be removed (e.g., previous versions) after updated versions have been installed.	DoD has defined the firmware components as all upgraded/replaced firmware components that are no longer required for operation.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the firmware components as all upgraded/replaced firmware components that are no longer required for operation.

SI-2 (6)	SI-2 (6)	CCI-002617	The organization removes organization-defined software components (e.g., previous versions) after updated versions have been installed.	The organization being inspected/assessed configures the information system to remove all upgraded/replaced software components that are no longer required for operation (e.g., previous versions) after updated versions have been installed. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2617. DoD has defined the software components as all upgraded/replaced software components that are no longer required for operation.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to remove all upgraded/replaced software components that are no longer required for operation (e.g., previous versions) after updated versions have been installed. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2617. DoD has defined the software components as all upgraded/replaced software components that are no longer required for operation.
SI-2 (6)	SI-2 (6)	CCI-002618	The organization removes organization-defined firmware components (e.g., previous versions) after updated versions have been installed.	The organization being inspected/assessed configures the information system to remove all upgraded/replaced firmware components that are no longer required for operation e.g., previous versions) after updated versions have been installed. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2618. DoD has defined the firmware components as all upgraded/replaced firmware components that are no longer required for operation.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to remove all upgraded/replaced firmware components that are no longer required for operation (e.g., previous versions) after updated versions have been installed. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2618. DoD has defined the firmware components as all upgraded/replaced firmware components that are no longer required for operation.
SI-3	SI-3 (a)	CCI-002619	The organization employs malicious code protection mechanisms at information system entry points to detect malicious code.	The organization being inspected/assessed identifies and documents the information system entry points and implements malicious code protection mechanisms at those entry points to detect malicious code. Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, notebook computers, and mobile devices. Malicious code protection mechanisms include, for example, anti-virus signature definitions and reputation-based technologies.	The organization conducting the inspection/assessment examines the information system architecture as well as the organization's documentation of information system entry points and verifies that malicious code protection mechanisms are implemented.
SI-3	SI-3 (a)	CCI-002621	The organization employs malicious code protection mechanisms at information system entry points to eradicate malicious code.	The organization being inspected/assessed configures the malicious code protection mechanisms identified in SI-3, CCI 2619 to eradicate malicious code.	The organization conducting the inspection/assessment examines the information system architecture as well as the organization's documentation of information system entry points and verifies that malicious code protection mechanisms are implemented to eradicate malicious code.
SI-3	SI-3 (a)	CCI-002620	The organization employs malicious code protection mechanisms at information system exit points to detect malicious code.	The organization being inspected/assessed identifies and documents the information system exit points and implements malicious code protection mechanisms at those exit points to detect malicious code. Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, notebook computers, and mobile devices. Malicious code protection mechanisms include, for example, anti-virus signature definitions and reputation-based technologies.	The organization conducting the inspection/assessment examines the information system architecture as well as the organization's documentation of information system exit points and verifies that malicious code protection mechanisms are implemented.
SI-3	SI-3 (a)	CCI-002622	The organization employs malicious code protection mechanisms at information system exit points to eradicate malicious code.	The organization being inspected/assessed configures the malicious code protection mechanisms identified in SI-3, CCI 2620 to eradicate malicious code.	The organization conducting the inspection/assessment examines the information system architecture as well as the organization's documentation of information system exit points and verifies that malicious code protection mechanisms are implemented to eradicate malicious code.

SI-3	SI-3 (b)	CCI-001240	The organization updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures.	The organization being inspected/assessed configures the information system to update malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1240.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to update malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1240.
SI-3	SI-3 (c) (1)	CCI-002623	The organization defines the frequency for performing periodic scans of the information system for malicious code.	DoD has defined the frequency as every 7 days.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every 7 days.
SI-3	SI-3 (c) (1)	CCI-002624	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.	The organization being inspected/assessed configures the 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. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2624.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed 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. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2624.
SI-3	SI-3 (c) (1)	CCI-001242	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.	The organization being inspected/assessed 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. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1242.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed 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. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1242.
SI-3	SI-3 (c) (1)	CCI-001241	The organization configures malicious code protection mechanisms to perform periodic scans of the information system on an organization-defined frequency.	The organization being inspected/assessed configures malicious code protection mechanisms to perform periodic scans of the information system on every 7 days. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1241. DoD has defined the frequency as every 7 days.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures malicious code protection mechanisms to perform periodic scans of the information system on every 7 days. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1241. DoD has defined the frequency as every 7 days.
SI-3	SI-3 (c) (2)	CCI-001244	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 alert to administrator.	DoD has defined the actions as block and quarantine malicious code and then send an alert to the administrator immediately in near real-time.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the actions as block and quarantine malicious code and then send an alert to the administrator immediately in near real-time.

SI-3	SI-3 (c) (2)	CCI-001243	The organization configures malicious code protection mechanisms to perform organization-defined action(s) in response to malicious code detection.	The organization being inspected/assessed configures malicious code protection mechanisms to perform block and quarantine malicious code and then send an alert to the administrator immediately in near real-time in response to malicious code detection. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1243. DoD has defined the actions as block and quarantine malicious code and then send an alert to the administrator immediately in near real-time.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures malicious code protection mechanisms to perform block and quarantine malicious code and then send an alert to the administrator immediately in near real-time in response to malicious code detection. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1243. DoD has defined the actions as block and quarantine malicious code and then send an alert to the administrator immediately in near real-time.
SI-3	SI-3 (d)	CCI-001245	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.	The organization being inspected/assessed configures the information system to address the receipt of false positives during malicious code detection and eradication, and the resulting potential impact on the availability of the information system. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1245.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to address the receipt of false positives during malicious code detection and eradication, and the resulting potential impact on the availability of the information system. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1245.
SI-3 (1)	SI-3 (1)	CCI-001246	The organization centrally manages malicious code protection mechanisms.	The organization being inspected/assessed documents and implements a process to centrally manage malicious code protection mechanisms.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed centrally manages malicious code protection mechanisms.
SI-3 (2)	SI-3 (2)	CCI-001247	The information system automatically updates malicious code protection mechanisms.	The organization being inspected/assessed configures the information system to automatically update malicious code protection mechanisms. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1247.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to automatically update malicious code protection mechanisms. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1247.
SI-3 (10)	SI-3 (10) (a)	CCI-002634	The organization defines the tools to be employed to analyze the characteristics and behavior of malicious code.	The organization being inspected/assessed defines and documents the tools to be employed to analyze the characteristics and behavior of malicious code. DoD has determined the tools are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented tools to ensure the organization being inspected/assessed defines the tools to be employed to analyze the characteristics and behavior of malicious code. DoD has determined the tools are not appropriate to define at the Enterprise level.
SI-3 (10)	SI-3 (10) (a)	CCI-002635	The organization defines the techniques to be employed to analyze the characteristics and behavior of malicious code.	The organization being inspected/assessed defines and documents the techniques to be employed to analyze the characteristics and behavior of malicious code. DoD has determined the techniques are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented techniques to ensure the organization being inspected/assessed defines the techniques to be employed to analyze the characteristics and behavior of malicious code. DoD has determined the techniques are not appropriate to define at the Enterprise level.
SI-3 (10)	SI-3 (10) (a)	CCI-002636	The organization employs organization-defined tools to analyze the characteristics and behavior of malicious code.	The organization being inspected/assessed documents and implements tools defined in SI-3 (10), CCI 2634 to analyze the characteristics and behavior of malicious code.	The organization conducting the inspection/assessment obtains and examines the documented tools to ensure the organization being inspected/assessed employs tools defined in SI-3 (10), CCI 2634 to analyze the characteristics and behavior of malicious code.
SI-3 (10)	SI-3 (10) (a)	CCI-002638	The organization employs organization-defined techniques to analyze the characteristics and behavior of malicious code.	The organization being inspected/assessed documents and implements techniques defined in SI-3 (10), CCI 2635 to analyze the characteristics and behavior of malicious code.	The organization conducting the inspection/assessment obtains and examines the documented techniques to ensure the organization being inspected/assessed employs techniques defined in SI-3 (10), CCI 2635 to analyze the characteristics and behavior of malicious code.

SI-3 (10)	SI-3 (10) (b)	CCI-002639	The organization incorporates the results from malicious code analysis into organizational incident response processes.	The organization being inspected/assessed incorporates the results from malicious code analysis into organizational incident response processes.	The organization conducting the inspection/assessment obtains and examines the organizational incident response processes to ensure the organization being inspected/assessed incorporates the results from malicious code analysis into organizational incident response processes.
SI-3 (10)	SI-3 (10) (b)	CCI-002640	The organization incorporates the results from malicious code analysis into organizational flaw remediation processes.	The organization being inspected/assessed incorporates the results from malicious code analysis into organizational flaw remediation processes.	The organization conducting the inspection/assessment obtains and examines the flaw remediation processes to ensure the organization being inspected/assessed incorporates the results from malicious code analysis into organizational flaw remediation processes.
SI-4	SI-4 (a) (1)	CCI-001253	The organization defines the objectives of monitoring for attacks and indicators of potential attacks on the information system.	DoD has defined the monitoring objectives as sensor placement and monitoring requirements within CJCSI 6510.01F.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the monitoring objectives as sensor placement and monitoring requirements within CJCSI 6510.01F.
SI-4	SI-4 (a) (1)	CCI-002641	The organization monitors the information system to detect attacks and indicators of potential attacks in accordance with organization-defined monitoring objectives.	The organization being inspected/assessed documents and implements a process to monitor the information system to detect attacks and indicators of potential attacks in accordance with sensor placement and monitoring requirements within CJCSI 6510.01F. The organization must maintain an audit trail of monitoring. DoD has defined the monitoring objectives as sensor placement and monitoring requirements within CJCSI 6510.01F.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of monitoring to ensure the organization being inspected/assessed monitors the information system to detect attacks and indicators of potential attacks in accordance with sensor placement and monitoring requirements within CJCSI 6510.01F.
SI-4	SI-4 (a) (2)	CCI-002642	The organization monitors the information system to detect unauthorized local connections.	The organization being inspected/assessed documents and implements a process to monitor the information system to detect unauthorized local connections. The organization must maintain an audit trail of monitoring.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of monitoring to ensure the organization being inspected/assessed monitors the information system to detect unauthorized local connections.
SI-4	SI-4 (a) (2)	CCI-002643	The organization monitors the information system to detect unauthorized network connections.	The organization being inspected/assessed documents and implements a process to monitor the information system to detect unauthorized network connections. The organization must maintain an audit trail of monitoring.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of monitoring to ensure the organization being inspected/assessed monitors the information system to detect unauthorized network connections.
SI-4	SI-4 (a) (2)	CCI-002644	The organization monitors the information system to detect unauthorized remote connections.	The organization being inspected/assessed documents and implements a process to monitor information system to detect unauthorized remote connections. The organization must maintain an audit trail of monitoring.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of monitoring to ensure the organization being inspected/assessed monitors the information system to detect unauthorized remote connections.
SI-4	SI-4 (b)	CCI-002645	The organization defines the techniques and methods to be used to identify unauthorized use of the information system.	The organization being inspected/assessed defines and documents the techniques and methods to be used to identify unauthorized use of the information system. DoD has determined the techniques and methods are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented techniques to ensure the organization being inspected/assessed defines the techniques and methods to be used to identify unauthorized use of the information system. DoD has determined the techniques and methods are not appropriate to define at the Enterprise level.
SI-4	SI-4 (b)	CCI-002646	The organization identifies unauthorized use of the information system through organization-defined techniques and methods.	The organization being inspected/assessed identifies unauthorized use of the information system through techniques and methods defined in SI-4, CCI 2645. The organization must maintain an audit trail of identified instances of unauthorized use.	The organization conducting the inspection/assessment obtains and examines the audit trail of identified instances of unauthorized use to ensure the organization being inspected/assessed identifies unauthorized use of the information system through techniques and methods defined in SI-4, CCI 2645.
SI-4	SI-4 (c)	CCI-001255	The organization deploys monitoring devices strategically within the information system to collect organization determined essential information.	The organization being inspected/assessed documents and implements a process to deploy monitoring devices strategically within the information system to collect organization determined essential information.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed deploys monitoring devices strategically within the information system to collect organization determined essential information.
SI-4	SI-4 (c)	CCI-001256	The organization deploys monitoring devices at ad hoc locations within the system to track specific types of transactions of interest to the organization.	The organization being inspected/assessed documents and implements a process to deploy monitoring devices at ad hoc locations within the system to track specific types of transactions of interest to the organization.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed deploys monitoring devices at ad hoc locations within the system to track specific types of transactions of interest to the organization.

SI-4	SI-4 (d)	CCI-002647	The organization protects information obtained from intrusion-monitoring tools from unauthorized access.	The organization being inspected/assessed documents and implements a process to protect information obtained from intrusion-monitoring tools from unauthorized access.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed protects information obtained from intrusion-monitoring tools from unauthorized access.
SI-4	SI-4 (d)	CCI-002648	The organization protects information obtained from intrusion-monitoring tools from unauthorized modification.	The organization being inspected/assessed documents and implements a process to protect information obtained from intrusion-monitoring tools from unauthorized modification.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed protects information obtained from intrusion-monitoring tools from unauthorized modification.
SI-4	SI-4 (d)	CCI-002649	The organization protects information obtained from intrusion-monitoring tools from unauthorized deletion.	The organization being inspected/assessed documents and implements a process to protect information obtained from intrusion-monitoring tools from unauthorized deletion.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed protects information obtained from intrusion-monitoring tools from unauthorized deletion.
SI-4	SI-4 (e)	CCI-001257	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.	The organization being inspected/assessed documents and implements a process to heighten 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.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed 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.
SI-4	SI-4 (f)	CCI-001258	The organization obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.	The organization being inspected/assessed obtains and documents legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.	The organization conducting the inspection/assessment obtains and examines the documented legal opinion to ensure the organization being inspected/assessed obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.
SI-4	SI-4 (g)	CCI-002650	The organization defines the information system monitoring information that is to be provided the organization-defined personnel or roles.	The organization being inspected/assessed defines and documents the information system monitoring information that is to be provided the organization-defined personnel or roles. DoD has determined the information system monitoring information is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented information system monitoring information to ensure the organization being inspected/assessed defines the information system monitoring information that is to be provided the organization-defined personnel or roles. DoD has determined the information system monitoring information is not appropriate to define at the Enterprise level.
SI-4	SI-4 (g)	CCI-002651	The organization defines the personnel or roles that are to be provided organization-defined information system monitoring information.	The organization being inspected/assessed defines and documents the personnel or roles that are to be provided organization-defined information system monitoring information. DoD has determined the personnel or roles are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented personnel or roles to ensure the organization being inspected/assessed defines the personnel or roles that are to be provided organization-defined information system monitoring information. DoD has determined the personnel or roles are not appropriate to define at the Enterprise level.
SI-4	SI-4 (g)	CCI-002652	The organization defines the frequency at which the organization will provide the organization-defined information system monitoring information to organization-defined personnel or roles	The organization being inspected/assessed defines and documents the frequency at which the organization will provide the organization-defined information system monitoring information to organization-defined personnel or roles DoD has determined the frequency is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented frequency to ensure the organization being inspected/assessed defines the frequency at which the organization will provide the organization-defined information system monitoring information to organization-defined personnel or roles. DoD has determined the frequency is not appropriate to define at the Enterprise level.
SI-4	SI-4 (g)	CCI-002654	The organization provides organization-defined information system monitoring information to organization-defined personnel or roles as needed or per organization-defined frequency.	The organization being inspected/assessed provides information system monitoring information defined in SI-4, CCI 2650 to personnel or roles defined in SI-4, CCI 2651 as needed or per the frequency defined in SI-4, CCI 2652. The organization must maintain an audit trail of when information is provided.	The organization conducting the inspection/assessment obtains and examines the audit trail of when information is provided to ensure the organization being inspected/assessed provides information system monitoring information defined in SI-4, CCI 2650 to personnel or roles defined in SI-4, CCI 2651 as needed or per the frequency defined in SI-4, CCI 2652.
SI-4 (1)	SI-4 (1)	CCI-002655	The organization connects individual intrusion detection tools into an information system-wide intrusion detection system.	The organization being inspected/assessed connects individual intrusion detection tools into an information system-wide intrusion detection system.	The organization conducting the inspection/assessment examines the information system-wide intrusion detection system architecture and individuals tools to ensure the organization being inspected/assessed connects individual intrusion detection tools into an information system-wide intrusion detection system.

SI-4 (1)	SI-4 (1)	CCI-002656	The organization configures individual intrusion detection tools into an information system-wide intrusion detection system.	The organization being inspected/assessed configures individual intrusion detection tools into an information system-wide intrusion detection system. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2656.	The organization conducting the inspection/assessment examines the information system-wide intrusion detection system to ensure the organization being inspected/assessed configures individual intrusion detection tools into an information system-wide intrusion detection system. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2656.
SI-4 (4)	SI-4 (4)	CCI-002659	The organization defines the frequency on which it will monitor inbound communications for unusual or unauthorized activities or conditions.	DoD has defined the frequency as continuously.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as continuously.
SI-4 (4)	SI-4 (4)	CCI-002660	The organization defines the frequency on which it will monitor outbound communications for unusual or unauthorized activities or conditions.	DoD has defined the frequency as continuously.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as continuously.
SI-4 (4)	SI-4 (4)	CCI-002661	The information system monitors inbound communications traffic per organization-defined frequency for unusual or unauthorized activities or conditions.	The organization being inspected/assessed configures the information system to monitor inbound communications traffic continuously for unusual or unauthorized activities or conditions. DoD has defined the frequency as continuously.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to monitor inbound communications traffic continuously for unusual or unauthorized activities or conditions. DoD has defined the frequency as continuously.
SI-4 (4)	SI-4 (4)	CCI-002662	The information system monitors outbound communications traffic per organization-defined frequency for unusual or unauthorized activities or conditions.	The organization being inspected/assessed configures the information system to monitor outbound communications traffic continuously for unusual or unauthorized activities or conditions. DoD has defined the frequency as continuously.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to monitor outbound communications traffic continuously for unusual or unauthorized activities or conditions. DoD has defined the frequency as continuously.
SI-4 (5)	SI-4 (5)	CCI-001264	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.	DoD has defined the compromise indicators as real time intrusion detection and when there are threats identified by authoritative sources (e.g. CTOs) and IAW incident categories I, II, IV, & VII within CJCSM 6510.01B.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the compromise indicators as real time intrusion detection and when there are threats identified by authoritative sources (e.g. CTOs) and IAW incident categories I, II, IV, & VII within CJCSM 6510.01B.
SI-4 (5)	SI-4 (5)	CCI-002663	The organization defines the personnel or roles to receive information system alerts when organization-defined indicators of compromise or potential compromise occur.	DoD has defined the personnel or roles as at a minimum, the ISSM and ISSO.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as at a minimum, the ISSM and ISSO.
SI-4 (5)	SI-4 (5)	CCI-002664	The information system alerts organization-defined personnel or roles when organization-defined compromise indicators reflect the occurrence of a compromise or a potential compromise.	The organization being inspected/assessed configures the information system to alert at a minimum, the ISSM and ISSO when real time intrusion detection and when there are threats identified by authoritative sources (e.g. CTOs) and IAW incident categories I, II, IV, & VII within CJCSM 6510.01B reflect the occurrence of a compromise or a potential compromise. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2664. DoD has defined the personnel or roles as at a minimum, the ISSM and ISSO. DoD has defined the compromise indicators as real time intrusion detection and when there are threats identified by authoritative sources (e.g. CTOs) and IAW incident categories I, II, IV, & VII within CJCSM 6510.01B.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to alert at a minimum, the ISSM and ISSO when real time intrusion detection and when there are threats identified by authoritative sources (e.g. CTOs) and IAW incident categories I, II, IV, & VII within CJCSM 6510.01B reflect the occurrence of a compromise or a potential compromise. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2664. DoD has defined the personnel or roles as at a minimum, the ISSM and ISSO. DoD has defined the compromise indicators as real time intrusion detection and when there are threats identified by authoritative sources (e.g. CTOs) and IAW incident categories I, II, IV, & VII within CJCSM 6510.01B.

SI-4 (11)	SI-4 (11)	CCI-002668	The organization defines the interior points within the information system (e.g., subnetworks, subsystems) where outbound communications will be analyzed to discover anomalies.	The organization being inspected/assessed defines and documents the interior points within the information system (e.g., subnetworks, subsystems) where outbound communications will be analyzed to discover anomalies. DoD has determined the interior points are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented interior points to ensure the organization being inspected/assessed defines the interior points within the information system (e.g., subnetworks, subsystems) where outbound communications will be analyzed to discover anomalies. DoD has determined the interior points are not appropriate to define at the Enterprise level.
SI-4 (11)	SI-4 (11)	CCI-001273	The organization analyzes outbound communications traffic at the external boundary of the information system to discover anomalies.	The organization being inspected/assessed documents and implements a process to analyze outbound communications traffic at the external boundary of the information system to discover anomalies. The organization must maintain a record of any discovered anomalies.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of any discovered anomalies to ensure the organization being inspected/assessed analyzes outbound communications traffic at the external boundary of the information system to discover anomalies.
SI-4 (11)	SI-4 (11)	CCI-001671	The organization analyzes outbound communications traffic at selected organization-defined interior points within the system (e.g., subnetworks, subsystems) to discover anomalies.	The organization being inspected/assessed documents and implements a process to analyze outbound communications traffic at selected interior points defined in SI-4 (11), CCI 2668 within the system (e.g., subnetworks, subsystems) to discover anomalies. The organization must maintain a record of any discovered anomalies.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of any discovered anomalies to ensure the organization being inspected/assessed analyzes outbound communications traffic at selected interior points defined in SI-4 (11), CCI 2668 within the system (e.g., subnetworks, subsystems) to discover anomalies.
SI-4 (12)	SI-4 (12)	CCI-001275	The organization defines the activities which will trigger alerts to security personnel of inappropriate or unusual activities.	DoD has defined the activities that trigger alerts as when there are threats identified by authoritative sources (e.g. CTOs) and IAW with CJCSM 6510.01B.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the activities that trigger alerts as when there are threats identified by authoritative sources (e.g. CTOs) and IAW with CJCSM 6510.01B.
SI-4 (12)	SI-4 (12)	CCI-001274	The organization employs automated mechanisms to alert security personnel of an organization-defined inappropriate or unusual activities with security implications.	The organization being inspected/assessed documents and implements automated mechanisms to alert security personnel when there are threats identified by authoritative sources (e.g. CTOs) and IAW with CJCSM 6510.01B. For automated alert mechanisms that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1274. DoD has defined the activities that trigger alerts as when there are threats identified by authoritative sources (e.g. CTOs) and IAW with CJCSM 6510.01B.	The organization conducting the inspection/assessment obtains and examines documentation of the use of the identified automated mechanisms used to alert security personnel when there are threats identified by authoritative sources (e.g. CTOs) and IAW with CJCSM 6510.01B. For automated alert mechanisms that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1274. The organization being inspected/assessed may be required to demonstrate use of their identified automated mechanisms. DoD has defined the activities that trigger alerts as when there are threats identified by authoritative sources (e.g. CTOs) and IAW with CJCSM 6510.01B.
SI-4 (14)	SI-4 (14)	CCI-001673	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.	The organization being inspected/assessed documents and implements a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system.	The organization conducting the inspection/assessment obtains and examines documentation of the use of the identified wireless intrusion detection system and the system hardware/software list to ensure the organization being inspected/assessed employs a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system. The organization being inspected/assessed may be required to demonstrate use of the wireless intrusion detection system.
SI-4 (15)	SI-4 (15)	CCI-001282	The organization employs an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks.	The organization being inspected/assessed documents and implements an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks.	The organization conducting the inspection/assessment obtains and examines documentation of the use of the identified intrusion detection system to ensure the organization being inspected/assessed employs an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks. The organization being inspected/assessed may be required to demonstrate use of the intrusion detection system.

SI-4 (16)	SI-4 (16)	CCI-001283	The organization correlates information from monitoring tools employed throughout the information system.	The organization being inspected/assessed documents and implements a process to correlate information from monitoring tools employed throughout the information system.	The organization conducting the inspection/assessment obtains and examines the documented process and the correlated results to ensure the organization being inspected/assessed correlates information from monitoring tools employed throughout the information system.
SI-4 (19)	SI-4 (19)	CCI-002673	The organization defines the additional monitoring to be implemented for individuals identified as posing an increased level of risk.	The organization being inspected/assessed defines and documents the additional monitoring to be implemented for individuals identified as posing an increased level of risk. DoD has determined the additional monitoring is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented additional monitoring to ensure the organization being inspected/assessed defines the additional monitoring to be implemented for individuals identified as posing an increased level of risk. DoD has determined the additional monitoring is not appropriate to define at the Enterprise level.
SI-4 (19)	SI-4 (19)	CCI-002674	The organization defines the sources that may be used to identify individuals who pose an increased level of risk.	The organization being inspected/assessed defines and documents the sources that may be used to identify individuals who pose an increased level of risk. DoD has determined the sources are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented sources to ensure the organization being inspected/assessed defines the sources that may be used to identify individuals who pose an increased level of risk. DoD has determined the sources are not appropriate to define at the Enterprise level.
SI-4 (19)	SI-4 (19)	CCI-002675	The organization implements organization-defined additional monitoring of individuals who have been identified by organization-defined sources as posing an increased level of risk.	The organization being inspected/assessed implements additional monitoring defined in SI-4 (19), CCI 2673 of individuals who have been identified by sources defined in SI-4 (19), CCI 2674 as posing an increased level of risk. The organization must maintain an audit trail of additional monitoring.	The organization conducting the inspection/assessment obtains and examines the audit trail of additional monitoring to ensure the organization being inspected/assessed implements additional monitoring defined in SI-4 (19), CCI 2673 of individuals who have been identified by sources defined in SI-4 (19), CCI 2674 as posing an increased level of risk.
SI-4 (20)	SI-4 (20)	CCI-002676	The organization defines additional monitoring to be implemented for privileged users.	The organization being inspected/assessed defines and documents additional monitoring to be implemented for privileged users. DoD has determined the additional monitoring is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented additional monitoring to ensure the organization being inspected/assessed defines additional monitoring to be implemented for privileged users. DoD has determined the additional monitoring is not appropriate to define at the Enterprise level.
SI-4 (20)	SI-4 (20)	CCI-002677	The organization implements organization-defined additional monitoring of privileged users.	The organization being inspected/assessed implements additional monitoring defined in SI-4 (20), CCI 2676 of privileged users. The organization must maintain an audit trail of additional monitoring.	The organization conducting the inspection/assessment obtains and examines the audit trail of additional monitoring to ensure the organization being inspected/assessed implements additional monitoring defined in SI-4 (20), CCI 2676 of privileged users.
SI-4 (22)	SI-4 (22)	CCI-002681	The organization defines the authorization or approval process for network services.	DoD has defined the personnel or roles as at a minimum, the ISSO and ISSM.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as at a minimum, the ISSO and ISSM.
SI-4 (22)	SI-4 (22)	CCI-002682	The organization defines the personnel or roles to be alerted when unauthorized or unapproved network services are detected.	DoD has defined the personnel or roles as at a minimum, the ISSO and ISSM.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as at a minimum, the ISSO and ISSM.
SI-4 (22)	SI-4 (22)	CCI-002683	The information system detects network services that have not been authorized or approved by the organization-defined authorization or approval processes.	The organization being inspected/assessed documents and implements a process to detect network services that have not been authorized or approved by at a minimum, the ISSO and ISSM. For network service detection mechanisms that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2683. DoD has defined the personnel or roles as at a minimum, the ISSO and ISSM.	The organization conducting the inspection/assessment obtains and examines the documented process, and examines the implemented detection mechnanisms to ensure the organization being inspected/assessed implements a process to detect network services that have not been authorized or approved by at a minimum, the ISSO and ISSM. For network service detection mechanisms that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2683. DoD has defined the personnel or roles as at a minimum, the ISSO and ISSM.

SI-4 (22)	SI-4 (22)	CCI-002684	The information system audits and/or alerts organization-defined personnel when unauthorized network services are detected.	The organization being inspected/assessed configures the information system to audit and/or alert at a minimum, the ISSO and ISSM when unauthorized network services are detected. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2684. DoD has defined the personnel or roles as at a minimum, the ISSO and ISSM.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to audit and/or alert at a minimum, the ISSO and ISSM when unauthorized network services are detected. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2684. DoD has defined the personnel or roles as at a minimum, the ISSO and ISSM.
SI-4 (23)	SI-4 (23)	CCI-002685	The organization defines the host-based monitoring mechanisms to be implemented at organization-defined information system components.	DoD has defined the host-based monitoring mechanisms as HBSS.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the host-based monitoring mechanisms as HBSS.
SI-4 (23)	SI-4 (23)	CCI-002686	The organization defines the information system components at which organization-defined host-based monitoring mechanisms are to be implemented.	DoD has defined the information system components as all components.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the information system components as all components.
SI-4 (23)	SI-4 (23)	CCI-002687	The organization implements organization-defined host-based monitoring mechanisms at organization-defined information system components.	The organization being inspected/assessed documents and implements HBSS at all components. DoD has defined the host-based monitoring mechanisms as HBSS. DoD has defined the information system components as all components.	The organization conducting the inspection/assessment obtains and examines documentation of the use of HBSS to ensure the organization being inspected/assessed implements HBSS at all components. The organization being inspected/assessed may be required to demonstrate use of HBSS. DoD has defined the host-based monitoring mechanisms as HBSS. DoD has defined the information system components as all components.
SI-5	SI-5 (a)	CCI-002692	The organization defines the external organizations from which it receives information system security alerts, advisories and directives.	DoD has defined the external organizations as at a minimum, USCYBERCOM.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the external organizations as at a minimum, USCYBERCOM.
SI-5	SI-5 (a)	CCI-001285	The organization receives information system security alerts, advisories, and directives from organization-defined external organizations on an ongoing basis.	The organization being inspected/assessed receives information system security alerts, advisories, and directives from at a minimum, USCYBERCOM on an ongoing basis. DoD has defined the external organizations as at a minimum, USCYBERCOM.	The organization conducting the inspection/assessment obtains and examines alerts, advisories, and directives received by the organization being inspected/assessed to ensure they receive information system security alerts, advisories, and directives from at a minimum, USCYBERCOM on an ongoing basis. DoD has defined the external organizations as at a minimum, USCYBERCOM.
SI-5	SI-5 (b)	CCI-001286	The organization generates internal security alerts, advisories, and directives as deemed necessary.	The organization being inspected/assessed documents and implements a process to generate internal security alerts, advisories, and directives as deemed necessary.	The organization conducting the inspection/assessment obtains and examines documented process as well as the generated internal security alerts, advisories, and directives to ensure the organization being inspected/assessed generates internal security alerts, advisories, and directives as deemed necessary.
SI-5	SI-5 (c)	CCI-001288	The organization defines the personnel or roles to whom the organization will disseminate security alerts, advisories and directives.	DoD has defined the personnel or roles as the ISSO and ISSM.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as the ISSO and ISSM.
SI-5	SI-5 (c)	CCI-002693	The organization defines the elements within the organization to whom the organization will disseminate security alerts, advisories and directives.	DoD has determined the elements are not applicable as elements are not selected as recipients of security alerts, advisories and directives.	DoD has determined the elements are not applicable as elements are not selected as recipients of security alerts, advisories and directives.
SI-5	SI-5 (c)	CCI-002694	The organization defines the external organizations to whom the organization will disseminate security alerts, advisories and directives.	DoD has defined the external organizations as CNDSP Tier 1 for vetting. The CNDSP Tier 1 will pass the information to the accredited Tier 2 CNDSPs. Tier 2 CNDSPs are responsible for ensuring all Tier 3 entities receive the information. Tier 3 organizations will ensure all local Op Centers/LAN shops receive information (i.e. Component IT System and Security Personnel) (e.g. ISSM, ISSOs, and system administrators).	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the external organizations as CNDSP Tier 1 for vetting. The CNDSP Tier 1 will pass the information to the accredited Tier 2 CNDSPs. Tier 2 CNDSPs are responsible for ensuring all Tier 3 entities receive the information. Tier 3 organizations will ensure all local Op Centers/LAN shops receive information (i.e. Component IT System and Security Personnel) (e.g. ISSM, ISSOs, and system administrators).

SI-5	SI-5 (c)	CCI-001287	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.	The organization being inspected/assessed disseminates security alerts, advisories, and directives to the ISSO and ISSM and/or external organizations defined in SI-5, CCI 2694. DoD has defined the personnel or roles as the ISSO and ISSM.	The organization conducting the inspection/assessment obtains and examines any applicable artifacts showing dissemination of security alerts, advisories, and directives to ensure the organization being inspected/assessed disseminates security alerts, advisories, and directives to the ISSO and ISSM and/or external organizations defined in SI-5, CCI 2694. DoD has defined the personnel or roles as the ISSO and ISSM.
SI-5	SI-5 (d)	CCI-001289	The organization implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.	The organization being inspected/assessed implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.	The organization conducting the inspection/assessment examines the information system and obtains and examines records of compliance and/or non-compliance reporting to ensure that security directives have been implemented in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.
SI-7 (14)	SI-7 (14) (a)	CCI-002737	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.	The organization being inspected/assessed prohibits the use of binary or machine-executable code obtained from sources without vendor support or with no warranty and without the provision of source code.	The organization conducting the inspection/assessment obtains and examines the software list and examines the information system to ensure the organization being inspected/assessed prohibits the use of binary or machine-executable code obtained from sources without vendor support or with no warranty and without the provision of source code.
SI-7 (14)	SI-7 (14) (b)	CCI-002738	The organization provides exceptions to the source code requirement only for compelling mission/operational requirements and with the approval of the authorizing official.	The organization being inspected/assessed documents and provides exceptions to the source code requirement only for compelling mission/operational requirements and with the approval of the authorizing official.	The organization conducting the inspection/assessment obtains and examines the documented exceptions to the source code requirement to ensure the organization being inspected/assessed provides justification and approval of the authorizing official for all exceptions to the source code requirement.
SI-10	SI-10	CCI-002744	The organization defines the inputs the information system is to conduct validity checks.	The organization being inspected/assessed defines and documents specific inputs which do not require validity checks. DoD has defined the information inputs as all inputs except those identified specifically by the organization.	The organization conducting the DoD has defined the information inputs as all inputs except those identified specifically by the organization.
SI-10	SI-10	CCI-001310	The information system checks the validity of organization-defined inputs.	The organization being inspected/assessed configures the information system to check the validity of all inputs except those identified specifically by the organization. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1310. DoD has defined the information inputs as all inputs except those identified specifically by the organization.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to check the validity of all inputs except those identified specifically by the organization. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1310. DoD has defined the information inputs as all inputs except those identified specifically by the organization.
SI-11	SI-11 (a)	CCI-001312	The information system generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries.	The organization being inspected/assessed configures the information system to generate error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1312.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to generate error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1312.
SI-11	SI-11 (b)	CCI-002759	The organization defines the personnel or roles to whom error messages are to be revealed.	DoD has defined the personnel or roles as the ISSO, ISSM, and SCA.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as the ISSO, ISSM, and SCA.

SI-11	SI-11 (b)	CCI-001314	The information system reveals error messages only to organization-defined personnel or roles.	The organization being inspected/assessed configures the information system to reveal error messages only to the ISSO, ISSM, and SCA. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1314. DoD has defined the personnel or roles as the ISSO, ISSM, and SCA.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to reveal error messages only to the ISSO, ISSM, and SCA. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1314. DoD has defined the personnel or roles as the ISSO, ISSM, and SCA.
SI-12	SI-12	CCI-001315	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.	The organization being inspected/assessed identifies and documents federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements which apply to the information within the information system. The organization documents and implements a process to handle information IAW those documented federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	The organization conducting the inspection/assessment obtains and examines the documented list of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements which apply to the information within the information system, as well as the documented process for information handling to ensure the organization being inspected/assessed 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.
SI-12	SI-12	CCI-001678	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.	The organization being inspected/assessed identifies and documents federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements which apply to the information within the information system. The organization documents and implements a process to retain information IAW those documented federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	The organization conducting the inspection/assessment obtains and examines the documented list of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements which apply to the information within the information system, as well as the documented process for information retention to ensure the organization being inspected/assessed 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.