| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **SC-13** | USE OF CRYPTOGRAPHY | |
| **SC-13.1**  **SC-13.1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system implements cryptographic protections using cryptographic modules that comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing use of cryptography; information system design documentation; information system configuration settings and associated documentation; cryptographic module validation certificates; other relevant documents or records]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6, IA-7, SC-12  successor controls: None |
| **Action Step** | | **Potential Assessor Evidence Gathering Actions**  **\*\*See “**[**Assessment Case Overview**](http://csrc.nist.gov/groups/SMA/fisma/assessment-cases-overview.html)**” for selecting, tailoring and executing action steps\*\*** |
|  | | *\*\*Assessment Case Assessor Note:* More convincing evidence (i.e., greater assurance) of correct implementation and operating as intended can be obtained through the assessment case actions by:   1. **Replacing bracketed values in action gathering statements to apply greater rigor in the assessment** (e.g, . replacing [“*reviewing*”] with “*studying*” or “*analyzing*”; replacing [“*observing*”] with “*inspecting*” or “*analyzing*”; replacing [“*basic*”] with “*focused*” or “*comprehensive*”); 2. **Replacing bracketed values in action gathering statements to apply greater sample coverage in the assessment** (e.g, . replacing [“*basic”*] sample with “*focused*” or “*sufficiently large”* sample); 3. **Defining additional action steps to the list of action steps suggested herein that exercise additional test methods** (i.e., Examine, Interview or Test) on additional assessment objects. |
| **SC-13.1.1.1** | | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the cryptographic modules and their configuration settings to be employed to implement cryptographic protections that comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. |
| **SC-13.1.1.2** | | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the cryptographic modules identified in SC-13.1.1.1; [*reviewing*] for evidence that these modules are configured as identified in SC-13.1.1.1. |
| **SC-13.1.1.3** | | **Test** an agreed-upon [*basic*] sample of the cryptographic modules and their configuration settings identified in SC-13.1.1.1; conducting [*basic*] testing for evidence that these modules are operating as intended. |
|  | | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 1** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SC-13(1)** | USE OF CRYPTOGRAPHY |
| **SC-13(1).1**  **SC-13(1).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization employs, at a minimum, FIPS-validated cryptography to protect unclassified information.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing use of cryptography; FIPS cryptography standards; information system design documentation; information system configuration settings and associated documentation; cryptographic module validation certificates; other relevant documents or records]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6, IA-7, SC-12  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SC-13(1).1.1.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the cryptographic mechanisms and their configuration settings to be employed to protect unclassified information using FIPS-validated cryptography. |
| **SC-13(1).1.1.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the cryptographic mechanisms identified in SC-13(1).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-13(1).1.1.1. |
| **SC-13(1).1.1.3** | **Test** an agreed-upon [*basic*] sample of the cryptographic mechanisms and their configuration settings identified in SC-13(1).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 2** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SC-13(2)** | USE OF CRYPTOGRAPHY |
| **SC-13(2).1**  **SC-13(2).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization employs NSA-approved cryptography to protect classified information.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing use of cryptography; NSA cryptography standards; information system design documentation; information system configuration settings and associated documentation; cryptographic module validation certificates; other relevant documents or records]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6, IA-7, SC-12  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SC-13(2).1.1.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the cryptographic mechanisms and their configuration settings to be employed to protect classified information using NSA-approved cryptography. |
| **SC-13(2).1.1.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the cryptographic mechanisms identified in SC-13(2).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-13(2).1.1.1. |
| **SC-13(2).1.1.3** | **Test** an agreed-upon [*basic*] sample of the cryptographic mechanisms and their configuration settings identified in SC-13(2).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 3** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SC-13(3)** | USE OF CRYPTOGRAPHY |
| **SC-13(3).1**  **SC-13(3).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization employs, at a minimum, FIPS-validated cryptography to protect information when such information must be separated from individuals who have the necessary clearances yet lack the necessary access approvals.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing use of cryptography; FIPS cryptography standards; information system design documentation; information system configuration settings and associated documentation; FIPS cryptographic module validation certificates; other relevant documents or records].  **Interview**:[*select from:* Organizational personnel with responsibilities for implementing cryptography within the information system]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6, IA-7, SC-12  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SC-13(3).1.1.1** | **Examine** system and communications protection policy, procedures addressing use of cryptography, security plan, or other relevant documents; [*reviewing*] for the situations when information must be separated from individuals who have the necessary clearances yet lack the necessary access approvals. |
| **SC-13(3).1.1.2** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the cryptographic mechanisms and their configuration settings to be employed to protect information for situations identified in SC-13(3).1.1.1. |
| **SC-13(3).1.1.3** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the cryptographic mechanisms identified in SC-13(3).1.1.2; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-13(3).1.1.2. |
| **SC-13(3).1.1.4** | **Test** an agreed-upon [*basic*] sample of the cryptographic mechanisms and their configuration settings identified in SC-13(3).1.1.2; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 4** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SC-13(4)** | USE OF CRYPTOGRAPHY |
| **SC-13(4).1**  **SC-13(4).1.1**  **SC-13(4).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines whether it will use NIST-approved or NSA-approved cryptography to implement digital signatures; and* 2. *the organization employs the organization-defined cryptography to implement digital signatures*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing use of cryptography; information system design documentation; information system configuration settings and associated documentation; cryptographic module validation certificates; other relevant documents or records]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6, IA-7, SC-12  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SC-13(4).1.1.1** | **Examine** system and communications protection policy, procedures addressing use of cryptography, security plan, or other relevant documents; [*reviewing*] for the cryptography (NIST-approved or NSA-approved) to be employed to implement digital signatures. |
|  |  |
| **SC-13(4).1.2.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the cryptographic mechanisms and their configuration settings to be employed to implement digital signatures using the cryptography identified in SC-13(4).1.1.1. |
| **SC-13(4).1.2.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the cryptographic mechanisms identified in SC-13(4).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-13(4).1.2.1. |
| **SC-13(4).1.2.3** | **Test** an agreed-upon [*basic*] sample of the cryptographic mechanisms and their configuration settings identified in SC-13(4).1.2.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |