| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **MA-4** | NON-LOCAL MAINTENANCE | |
| **MA-4.1**  **MA-4.1.1**  **MA-4.1.2**  **MA-4.1.3**  **MA-4.1.4**  **MA-4.1.5**  **MA-4.1.6** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization authorizes, monitors, and controls non-local maintenance and diagnostic activities;* 2. *the organization documents, in the organizational policy and security plan for the information system, the acceptable conditions for allowing the use of non-local maintenance and diagnostic tools;* 3. *the organization allows the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and as documented in the security plan;* 4. *the organization employs strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions;* 5. *the organization maintains records for non-local maintenance and diagnostic activities; and* 6. *the organization (or information system in certain cases) terminates all sessions and network connections when non-local maintenance or diagnostics is completed.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Information system maintenance policy; procedures addressing non-local maintenance for the information system; security plan; information system design documentation; information system configuration settings and associated documentation; maintenance records; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with information system maintenance responsibilities]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AU-2, AU-3, AU-14, CM-2, MA-2  concurrent controls: AC-2, AC-3, AC-17, AC-18, AC-19, CM-3, CM-6, IA-2, IA-8, MA-3, MA-5,  MP-6, PL-4, PS-2, PS-3, PS-6, PS-7, SC-7, SC-10, SI-4  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. |
| **MA-4.1.1.1** | | **Examine** information system maintenance policy, procedures addressing non-local maintenance for the information system, security plan, or other relevant documents; [*reviewing*] for the measures (including automated mechanisms and their configuration settings) to be employed to authorize, monitor, and control non-local maintenance and diagnostic activities. |
| **MA-4.1.1.2** | | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in MA-4.1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in MA-4.1.1.1. |
| **MA-4.1.1.3** | | **Examine** access authorizations, service level agreements, maintenance schedules, maintenance records, diagnostic records, maintenance activity reviews, remote access control records, change control records, information system monitoring records, information system audit records, or other relevant documents for an agreed-upon [*basic*] sample of non-local maintenance and diagnostic activities; [*reviewing*] for evidence that the measures identified in MA-4.1.1.1 are being applied. |
| **MA-4.1.1.4** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with information system maintenance responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in MA-4.1.1.1 are being applied. |
| **MA-4.1.1.5** | | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in MA-4.1.1.1; conducting [*basic*] testing using simulated events or conditions for evidence that these mechanisms are operating as intended. |
|  | |  |
| **MA-4.1.2.1** | | **Examine** information system maintenance policy and security plan; [*reviewing*] for the acceptable conditions in which non-local maintenance and diagnostic tools are allowed to be used. |
|  | |  |
| **MA-4.1.3.1** | | **Examine** information system maintenance policy, procedures addressing non-local maintenance for the information system, security plan, or other relevant documents; [*reviewing*] for the non-local maintenance and diagnostic tools to be used consistent with the conditions identified in MA-4.1.2.1. |
| **MA-4.1.3.2** | | **Examine** maintenance records, remote access control records, change control records, information system monitoring records, information system audit records, or other relevant records for an agreed-upon [*basic*] sample of non-local maintenance and diagnostic activities; [*reviewing*] for evidence that only the tools identified in MA-4.1.3.1 are being used consistent with the conditions identified in MA-4.1.2.1. |
| **MA-4.1.3.3** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with information system maintenance responsibilities; conducting [*basic*] discussions for further evidence that only the tools identified in MA-4.1.3.1 are being used consistent with the conditions identified in MA-4.1.2.1. |
|  | |  |
| **MA-4.1.4.1** | | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to enforce strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions. |
| **MA-4.1.4.2** | | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in MA-4.1.4.1; [*reviewing*] for evidence that these mechanisms are configured as identified in MA-4.1.4.1. |
| **MA-4.1.4.3** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with information system maintenance responsibilities; conducting [*basic*] discussions for further evidence that the mechanisms and configurations identified in MA-4.1.4.1 are being applied. |
| **MA-4.1.4.4** | | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in MA-4.1.4.1; conducting [*basic*] testing using simulated events or conditions for evidence that these mechanisms are operating as intended. |
|  | |  |
|  | |  |
| **MA-4.1.5.1** | | **Examine** information system maintenance policy, procedures addressing non-local maintenance for the information system, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to maintain records for non-local maintenance and diagnostic activities. |
| **MA-4.1.5.2** | | **Examine** an agreed-upon [*basic*] sample of information system maintenance logs for non-local maintenance and diagnostic activities; [*reviewing*] for evidence that the measures identified in MA-4.1.5.1 are being applied to maintain records for non-local maintenance and diagnostic activities. |
| **MA-4.1.5.3** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with information system maintenance responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in MA-4.1.5.1 are being applied. |
|  | |  |
| **MA-4.1.6.1** | | **Examine** information system maintenance policy, procedures addressing non-local maintenance for the information system, security plan, information system design documentation, or other relevant documents; [*reviewing*] for the measures (including automated mechanisms and their configuration settings) to be employed to terminate all sessions and network connections when non-local maintenance or diagnostics is completed. |
| **MA-4.1.6.2** | | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in MA-4.1.6.1; [*reviewing*] for evidence that these mechanisms are configured as identified in MA-4.1.6.1. |
| **MA-4.1.6.3** | | **Examine** an agreed-upon [*basic*] sample of maintenance records, remote disconnect verification records, session termination records, session audit records, information system audit records, or other relevant information system records for an agreed-upon [*basic*] sample of completed non-local maintenance and diagnostic activities; [*reviewing*] for evidence that the mechanisms and configurations identified in MA-4.1.6.1 are being applied. |
| **MA-4.1.6.4** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with information system maintenance responsibilities; conducting [*basic*] discussions for further evidence that the mechanisms and configurations identified in MA-4.1.6.1 are being applied. |
| **MA-4.1.6.5** | | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in MA-4.1.6.1; conducting [*basic*] testing using simulated events or conditions for evidence that these mechanisms are operating as intended. |
|  | | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 1** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **MA-4(1)** | NON-LOCAL MAINTENANCE |
| **MA-4(1).1**  **MA-4(1).1.1**  **MA-4(1).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization audits non-local maintenance and diagnostic sessions; and* 2. *designated organizational personnel review the maintenance records of the sessions.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Information system maintenance policy; procedures addressing non-local maintenance for the information system; maintenance records; audit records; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with information system maintenance responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AU-2, AU-3, MA-2  concurrent controls: AC-17, AC-18, AU-6, AU-14, MA-3, MA-5, PS-2, PS-3, PS-7, SC-7  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **MA-4(1).1.1.1** | **Examine** information system maintenance policy, procedures addressing non-local maintenance for the information system, security plan, information system design documentation, or other relevant documents; [*reviewing*] for the measures (including automated mechanisms and their configuration settings) to be employed to audit non-local maintenance and diagnostic sessions. |
| **MA-4(1).1.1.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in MA-4(1).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in MA-4(1).1.1.1. |
| **MA-4(1).1.1.3** | **Examine** an agreed-upon [*basic*] sample of maintenance records, information system audit records, remote session logs, remote session records, remote access control records, or other relevant documents; [*reviewing*] for evidence that the measures identified in MA-4(1).1.1.1 are being applied. |
|  |  |
| **MA-4(1).1.2.1** | **Examine** information system maintenance policy, procedures addressing non-local maintenance for the information system, security plan, or other relevant documents; [*reviewing*] for the organizational personnel designated to review maintenance records of non-local maintenance and diagnostic sessions. |
| **MA-4(1).1.2.2** | **Examine** an agreed-upon [*basic*] sample of maintenance record reviews, information system audit record reviews, remote session log reviews, or other relevant documents; [*reviewing*] for evidence that the personnel designated in MA-4(1).1.2.1 review the maintenance records of non-local maintenance and diagnostic sessions. |
| **MA-4(1).1.2.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel identified in MA-4(1).1.2.1; conducting [*basic*] discussions for further evidence that these individuals review the maintenance records of non-local maintenance and diagnostic sessions. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 2** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **MA-4(2)** | NON-LOCAL MAINTENANCE |
| **MA-4(2).1**  **MA-4(2).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization documents the installation and use of non-local maintenance and diagnostic connections in the security plan for the information system.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Information system maintenance policy; procedures addressing non-local maintenance for the information system; security plan; maintenance records; audit records; other relevant documents or records]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: MA-2  concurrent controls: AC-4, AC-17, AC-18, CA-3, IA-3, SC-7  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **MA-4(2).1.1.1** | **Examine** security plan; [*reviewing*] for evidence that the plan documents the installation and use of non-local maintenance and diagnostic connections for the information system. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 3** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **MA-4(3)** | NON-LOCAL MAINTENANCE |
| **MA-4(3).1**  **MA-4(3).1.1**  **MA-4(3).1.2**  **MA-4(3).1.3** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization requires and ensures non-local maintenance and diagnostic services are performed from an information system that implements a level of security at least as high as the level of security implemented on the information system being serviced; or* 2. *the organization 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; and* 3. *the organization after the removed component service is performed, inspects and sanitizes the component (with regard to potentially malicious software and surreptitious implants) before reconnecting to the information system.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Information system maintenance policy; procedures addressing non-local maintenance for the information system; service provider contracts and/or service level agreements; maintenance records; audit records; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with information system maintenance responsibilities; information system maintenance provider]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: MA-2  concurrent controls: MA-3, MA-5, MP-6, SI-3  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **MA-4(3).1.1.1** | **Examine** information system maintenance policy, procedures addressing non-local maintenance for the information system, security plan, or other relevant documents; [*reviewing*] for the requirement that non-local maintenance and diagnostic services are to be performed from an information system that implements a level of security at least as high as the level of security implemented on the information system being serviced. |
| **MA-4(3).1.1.2** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with information system maintenance responsibilities; conducting [*basic*] discussions for further evidence of the requirement identified in MA-4(3).1.1.1. |
|  |  |
| **MA-4(3).1.2.1** | **Examine** information system maintenance policy, procedures addressing non-local maintenance for the information system, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to remove the component to be serviced from the information system and, prior to non-local maintenance or diagnostic services, sanitize the component (with regard to organizational information) before removal from organizational facilities. |
| **MA-4(3).1.2.2** | **Examine** service level agreements, equipment removal records, equipment sanitization records, media sanitization records, or other relevant documents for an agreed-upon [*basic*] sample of information system components removed from organizational facilities for maintenance and diagnostic services; [*reviewing*] for evidence that the measures identified in MA-4(3).1.2.1 are being applied. |
| **MA-4(3).1.2.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with information system maintenance responsibilities; conducting [*basic*] discussions for evidence that the measures identified in MA-4(3).1.2.1 are being applied. |
|  |  |
| **MA-4(3).1.3.1** | **Examine** information system maintenance policy, procedures addressing non-local maintenance for the information system, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to inspect and sanitize components, removed for service, (with regard to potentially malicious software and surreptitious implants) before reconnecting the components to their information system. |
| **MA-4(3).1.3.2** | **Examine** inspection records, results of malicious code checks, equipment sanitization records, media sanitization records, or other relevant documents for an agreed-upon [*basic*] sample of information system components removed for servicing; [*reviewing*] for evidence that the measures identified in MA-4(3).1.3.1 are being applied. |
| **MA-4(3).1.3.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with information system maintenance responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in MA-4(3).1.3.1 are being applied. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 4** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **MA-4(4)** | NON-LOCAL MAINTENANCE |
| **MA-4(4).1**  **MA-4(4).1.1**  **MA-4(4).1.2**  **MA-4(4).1.2a**  **MA-4(4).1.2b** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization protects non-local maintenance sessions through the use of a strong authenticator tightly bound to the user; and* 2. *the organization protects non-local maintenance sessions by separating the maintenance session from other network sessions with the information system by:*    * *either physically separated communications paths; or*    * *logically separated communications paths based upon encryption.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Information system maintenance policy; procedures addressing non-local maintenance for the information system; information system design documentation; information system configuration settings and associated documentation; maintenance records; audit records; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with information system maintenance responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: MA-2, CM-5  concurrent controls: AC-2, AC-3, AC-4, AC-17, AC-18, CM-6, IA-2, IA-3, IA-4, IA-5, IA-8,  PE-2, PE-3, SC-7, SC-13  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **MA-4(4).1.1.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to protect non-local maintenance sessions through the use of a strong authenticator tightly bound to the user. |
| **MA-4(4).1.1.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample the automated mechanisms identified in MA-4(4).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in MA-4(4).1.1.1. |
| **MA-4(4).1.1.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with information system maintenance responsibilities; conducting [*basic*] discussions for further evidence that the mechanisms and configurations identified in MA-4(4).1.1.1 are being applied. |
| **MA-4(4).1.1.4** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in MA-4(4).1.1.1; conducting [*basic*] testing using simulated events or conditions for evidence that these mechanisms are operating as intended. |
|  |  |
| **MA-4(4).1.2.1**  **MA-4(4).1.2.1.a**  **MA-4(4).1.2.1.b** | **Examine** information system maintenance policy, procedures addressing non-local maintenance for the information system, security plan, information system design documentation, or other relevant documents; [*reviewing*] for the measures (including automated mechanisms and their configuration settings) to be employed to separate maintenance sessions from other network sessions with the information system by:   * either physically separated communication paths; or * logically separated communications paths based upon encryption. |
| **MA-4(4).1.2.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in MA-4(4).1.2.1.a; [*reviewing*] for evidence that these mechanisms are configured as identified in MA-4(4).1.2.1.a to physically separate maintenance sessions from other network sessions with the information system. |
| **MA-4(4).1.2.3** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in MA-4(4).1.2.1.b; [*reviewing*] for evidence that these mechanisms are configured as identified in MA-4(4).1.2.1.b to logically separate maintenance sessions from other network sessions with the information system. |
| **MA-4(4).1.2.4** | **Examine** information system facilities; [*observing*] for evidence that the measures identified in MA-4(4).1.2.1.a are being applied to physically separate maintenance sessions from other network sessions with the information system. |
| **MA-4(4).1.2.5** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with information system maintenance responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in MA-4(4).1.2.1.a are being applied to physically separate maintenance sessions from other network sessions with the information system. |
| **MA-4(4).1.2.6** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with information system maintenance responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in MA-4(4).1.2.1.a are being applied to logically separate maintenance sessions from other network sessions with the information system. |
| **MA-4(4).1.2.7** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in MA-4(4).1.2.1.a; conducting [*basic*] testing using simulated events or conditions for evidence that these mechanisms are operating as intended to physically separate maintenance sessions from other network sessions for the information system. |
| **MA-4(4).1.2.8** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in MA-4(4).1.2.1.b; conducting [*basic*] testing using simulated events or conditions for evidence that these mechanisms are operating as intended to logically separate maintenance sessions from other network sessions for the information system. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 5** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **MA-4(5)** | NON-LOCAL MAINTENANCE |
| **MA-4(5).1**  **MA-4(5).1.1**  **MA-4(5).1.2**  **MA-4(5).1.3** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the organizational personnel to be notified when non-local maintenance is planned;* 2. *the organization requires that maintenance personnel notify organization-defined personnel when non-local maintenance is planned (i.e., date/time); and* 3. *the organization requires that a designated organizational official with specific information security/information system knowledge approves the non-local maintenance.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Information system maintenance policy; procedures addressing non-local maintenance for the information system; security plan; maintenance records; audit records; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with information system maintenance responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: CM-3, MA-2  concurrent controls: MA-5, PS-7  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **MA-4(5).1.1.1** | **Examine** information system maintenance policy, procedures addressing non-local maintenance for the information system, security plan, or other relevant documents; [*reviewing*] for the organizational personnel (identified by name or job position) to be notified when non-local maintenance is planned (i.e., date/time). |
|  |  |
| **MA-4(5).1.2.1** | **Examine** information system maintenance policy, procedures addressing non-local maintenance for the information system, security plan, or other relevant documents; [*reviewing*] for the requirement that maintenance personnel are to notify the personnel identified in MA-4(5).1.1.1 when non-local maintenance is planned (i.e., date/time). |
| **MA-4(5).1.2.2** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with information system maintenance responsibilities and organizational personnel identified MA-4(5).1.1.1; conducting [*basic*] discussions for further evidence of the requirement identified in MA-4(5).1.2.1. |
|  |  |
| **MA-4(5).1.3.1** | **Examine** information system maintenance policy, procedures addressing non-local maintenance for the information system, security plan, or other relevant documents; [*reviewing*] for the requirement that a designated organizational official with specific information security/information system knowledge approves non-local maintenance. |
| **MA-4(5).1.3.2** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with information system maintenance responsibilities and/or organizational personnel responsible for approving non-local maintenance; conducting [*basic*] discussions for further evidence of the requirement identified in MA-4(5).1.3.1. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 6** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **MA-4(6)** | NON-LOCAL MAINTENANCE |
| **MA-4(6).1**  **MA-4(6).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization employs cryptographic mechanisms to protect the integrity and confidentiality of non-local maintenance and diagnostic communications.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Information system maintenance policy; procedures addressing non-local maintenance for the information system; cryptographic mechanisms supporting information system maintenance activities; information system design documentation; information system configuration settings and associated documentation; maintenance records; audit records; other relevant documents or records].  **Test**: [*select from:* Cryptographic mechanisms supporting information system maintenance activities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: MA-2  concurrent controls: AC-3, AC-4, AC-17, AC-18, CM-6, SC-7, SC-8, SC-9, SC-13  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **MA-4(6).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 the integrity and confidentiality of non-local maintenance and diagnostic communications. |
| **MA-4(6).1.1.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the cryptographic mechanisms identified in MA-4(6).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in MA-4(6).1.1.1. |
| **MA-4(6).1.1.3** | **Examine** an agreed-upon [*basic*] sample of maintenance records, network communications records, information system audit records, or other relevant information system records for an agreed-upon [*basic*] sample of non-local maintenance and diagnostic communications activities; [*reviewing*] for evidence that the mechanisms and configurations identified in MA-4(6).1.1.1 are being applied. |
| **MA-4(6).1.1.4** | **Test** an agreed-upon [*basic*] sample of the cryptographic mechanisms and their configuration settings identified in MA-4(6).1.1.1; conducting [*basic*] testing using simulated events or conditions for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 7** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **MA-4(7)** | NON-LOCAL MAINTENANCE |
| **MA-4(7).1**  **MA-4(7).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization employs remote disconnect verification at the termination of non-local maintenance and diagnostic sessions.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Information system maintenance policy; procedures addressing non-local maintenance for the information system; information system design documentation; information system configuration settings and associated documentation; maintenance records; audit records; other relevant documents or records]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AU-2, AU-3, AU-14, MA-2  concurrent controls: AC-2, AC-3, AC-4, AC-10, AC-17, AC-18, CM-6, SC-10  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **MA-4(7).1.1.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to enforce remote disconnect verification at the termination of non-local maintenance and diagnostic sessions. |
| **MA-4(7).1.1.2** | **Examine** documentation describing the current configuration settings for agreed-upon [*basic*] sample of the automated mechanisms identified in MA-4(7).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in MA-4(7).1.1.1. |
| **MA-4(7).1.1.3** | **Examine** an agreed-upon [*basic*] sample of maintenance records, remote disconnect verification records, session termination records, session audit records, information system audit records, or other relevant information system records for an agreed-upon [*basic*] sample of non-local maintenance and diagnostic activities; [*reviewing*] for evidence that the mechanisms and configurations identified in MA-4(7).1.1.1 are being applied. |
| **MA-4(7).1.1.4** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with information system maintenance responsibilities; conducting [*basic*] discussions for further evidence that the mechanisms and configurations identified in MA-4(7).1.1.1 are being applied. |
| **MA-4(7)1..1.5** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in MA-4(7).1.1.1; conducting [*basic*] testing using simulated events or conditions for evidence that these mechanisms are operating as intended. |