| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **MA-5** | MAINTENANCE PERSONNEL | |
| **MA-5.1**  **MA-5.1.1**  **MA-5.1.2**  **MA-5.1.3** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization establishes a process for maintenance personnel authorization;* 2. *the organization maintains a current list of authorized maintenance organizations or personnel; and* 3. *personnel performing maintenance on the information system either have the required access authorizations or are supervised by designated organizational personnel with the required access authorizations and technical competence deemed necessary to supervise information system maintenance.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Information system maintenance policy; procedures addressing maintenance personnel; service provider contracts and/or service level agreements; list of authorized personnel; maintenance records; access control 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  concurrent controls: AC-2, AC-3, CM-5, IA-8, MA-4, PE-2, PE-3, PL-4, PS-2, PS-3,  PS-6, PS-7  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-5.1.1.1** | | **Examine** information system maintenance policy, procedures addressing maintenance personnel, security plan, or other relevant documents; [*reviewing*] for the process established for maintenance personnel authorization. |
| **MA-5.1.1.2** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with information system maintenance responsibilities; conducting [*basic*] discussions for further evidence of the process identified in MA-5.1.1.1. |
|  | |  |
| **MA-5.1.2.1** | | **Examine** maintenance authorizations associated with the process identified in MA-5.1.1.1; [*reviewing*] for a current list of authorized maintenance organizations or personnel. |
|  | |  |
| **MA-5.1.3.1** | | **Examine** the process identified in MA-5.1.1.1; [*reviewing*] for the measures to be employed to ensure that personnel performing maintenance on the information system have the required access authorizations. |
| **MA-5.1.3.2** | | **Examine** the process identified in MA-5.1.1.1; [*reviewing*] for the maintenance personnel who do not possess the required access authorizations to perform information system maintenance without supervision. |
| **MA-5.1.3.3** | | **Examine** the process identified in MA-5.1.1.1; [*reviewing*] for the designated organizational personnel with required access authorizations and technical competence deemed necessary to supervise information system maintenance performed by the maintenance personnel identified in MA-5.1.3.2. |
| **MA-5.1.3.4** | | **Examine** access authorizations for an agreed-upon [*basic*] sample of maintenance personnel identified in maintenance records for the information system; [*reviewing*] for evidence that the measures identified in MA-5.1.3.1 are being applied to ensure personnel performing maintenance on the information system have the required access authorizations. |
| **MA-5.1.3.5** | | **Examine** an agreed-upon [*basic*] sample of maintenance records for information system maintenance performed by an agreed-upon [*basic*] sample of maintenance personnel identified in MA-5.1.3.2; [*reviewing*] for evidence that the organizational personnel designated in MA-5.1.3.3 supervise information system maintenance when maintenance personnel do not possess the required access authorizations. |
| **MA-5.1.3.6** | | **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-5.1.3.1 are being applied to ensure personnel performing maintenance on the information system have the required access authorizations. |
| **MA-5.1.3.7** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel identified in MA-5.1.3.3; conducting [*basic*] discussions for further evidence that these individuals have the required access authorizations and technical competence deemed necessary to supervise information system maintenance performed by the maintenance personnel identified in MA-5.1.3.2. |
|  | | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 1** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **MA-5(1)** | **MAINTENANCE PERSONNEL** |
| **MA-5(1).1**  **MA-5(1).1.1**  **MA-5(1).1.1a**  **MA-5(1).1.1b**  **MA-5(1).1.1c** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization maintains procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements:*   * *maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified;* * *prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances, or formal access approvals, all volatile information storage components within the information system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and* * *in the event an information system component cannot be sanitized, the procedures contained in the security plan for the system are enforced.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Information system maintenance policy; procedures addressing maintenance personnel; information system media protection policy; physical and environmental protection policy; security plan; list of maintenance personnel requiring escort/supervision; maintenance records; access control records; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with information system maintenance responsibilities; organizational personnel with personnel security responsibilities; organizational personnel with physical access control responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: MA-2  concurrent controls: AC-2, AC-3, MP-2, MP-6, PE-2, PE-3, PL-4, PS-2, PS-3, PS-6,  PS-7  successor controls: None |

|  |  |
| --- | --- |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **MA-5(1).1.1.1**  **MA-5(1).1.1.1.a**  **MA-5(1).1.1.1.b**  **MA-5(1).1.1.1.c** | **Examine** information system maintenance policy, information system media protection policy, personnel security policy, physical and environmental protection policy, procedures addressing maintenance personnel, procedures addressing media sanitization and disposal, procedures addressing physical access authorizations, security plan, or other relevant documents; [*reviewing*] for the following requirements regarding the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens:   * + maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified;   + prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances, or formal access approvals, all volatile information storage components within the information system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and   + in the event an information system component cannot be sanitized, the procedures contained in the security plan for the system are enforced. |
| **MA-5(1).1.1.2** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with information system maintenance responsibilities, organizational personnel with information system media protection responsibilities, organizational personnel with personnel security responsibilities, and/or organizational personnel with physical access control responsibilities; conducting [*basic*] discussions for further evidence of the requirements identified in MA-5(1).1.1.1. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 2** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **MA-5(2)** | **MAINTENANCE PERSONNEL** |
| **MA-5(2).1**  **MA-5(2).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if personnel performing maintenance and diagnostic activities on an information system processing, storing, or transmitting classified information are cleared for the highest level of information on the system.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Information system maintenance policy; procedures addressing maintenance personnel; maintenance records; access control records; access authorizations; access credentials; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with information system maintenance responsibilities; organizational personnel with personnel security responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: MA-2  concurrent controls: AC-2, AC-3, PE-2, PE-3, PL-4, PS-2, PS-3, PS-6, PS-7  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **MA-5(2).1.1.1** | **Examine** information system maintenance policy, personnel security policy, physical and environmental protection policy, procedures addressing maintenance personnel, procedures addressing personnel security, procedures addressing physical access authorizations, security plan, or other relevant documents; [*reviewing*] for the highest level of classified information that the information system processes, stores, or transmits. |
| **MA-5(2).1.1.2** | **Examine** information system maintenance policy, personnel security policy, physical and environmental protection policy, procedures addressing maintenance personnel, procedures addressing personnel security, procedures addressing physical access authorizations, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to ensure personnel performing maintenance and diagnostic activities on the information system processing, storing, or transmitting classified information are cleared for the level identified in MA-5(2).1.1.1. |
| **MA-5(2).1.1.3** | **Examine** security clearances (or personnel screening records as appropriate) and an agreed-upon [*basic*] sample of maintenance records for an agreed-upon [*basic*] sample of personnel performing maintenance and diagnostic activities on the information system; [*reviewing*] for evidence that the measures identified in MA-5(2).1.1.2 are being applied. |
| **MA-5(2).1.1.4** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with information system maintenance responsibilities, organizational personnel with personnel security responsibilities, and/or organizational personnel with physical access control responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in MA-5(2).1.1.2 are being applied. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 3** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **MA-5(3)** | **MAINTENANCE PERSONNEL** |
| **MA-5(3).1**  **MA-5(3).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if personnel performing maintenance and diagnostic activities on the information system processing, storing, or transmitting classified information are U.S. citizens.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Information system maintenance policy; procedures addressing maintenance personnel; maintenance records; access control records; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with information system maintenance responsibilities, organizational personnel with personnel security responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: MA-2  concurrent controls: AC-2, AC-3, PE-2, PE-3, PL-4, PS-2, PS-3, PS-6, PS-7  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **MA-5(3).1.1.1** | **Examine** information system maintenance policy, personnel security policy, physical and environmental protection policy, procedures addressing maintenance personnel, procedures addressing personnel security, procedures addressing physical access authorizations, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to ensure personnel performing maintenance and diagnostic activities on the information system processing, storing, or transmitting classified information are U.S. citizens. |
| **MA-5(3).1.1.2** | **Examine** security clearances (or personnel screening records as appropriate) and an agreed-upon [*basic*] sample of maintenance records for an agreed-upon [*basic*] sample of personnel performing maintenance and diagnostic activities on the information system; [*reviewing*] for evidence that the measures identified in MA-5(3).1.1.1 are being applied. |
| **MA-5(3).1.1.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with information system maintenance responsibilities, organizational personnel with personnel security responsibilities, and/or organizational personnel with physical access control responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in MA-5(3).1.1.1 are being applied. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 4** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **MA-5(4)** | **MAINTENANCE PERSONNEL** |
| **MA-5(4).1**  **MA-5(4).1.1**  **MA-5(4).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *cleared foreign nationals are used to conduct maintenance and diagnostic activities on an information system only when the system is jointly owned and operated by the United States and foreign allied governments, or owned and operated solely by foreign allied governments; and* 2. *the organization documents in a Memorandum of Agreement the approvals, consents, and detailed operational conditions under which foreign nationals are allowed to conduct maintenance and diagnostic activities on an information system.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Information system maintenance policy; procedures addressing maintenance personnel; information system media protection policy; access control policy and procedures; physical and environmental protection policy and procedures; memorandum of agreement; maintenance records; access control records; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with information system maintenance responsibilities, organizational personnel with personnel security responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: MA-2  concurrent controls: AC-2, AC-3, PE-2, PE-3, PL-4, PS-2, PS-3, PS-6, PS-7  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **MA-5(4).1.1.1** | **Examine** information system maintenance policy, personnel security policy, physical and environmental protection policy, procedures addressing maintenance personnel, procedures addressing personnel security, procedures addressing physical access authorizations, security plan, or other relevant documents; [*reviewing*] for the cleared foreign nationals to be used to conduct maintenance and diagnostic activities on the information system only when the system is jointly owned and operated by the United States and foreign allied governments, or owned and operated solely by foreign allied governments. |
| **MA-5(4).1.1.2** | **Examine** information system maintenance policy, personnel security policy, physical and environmental protection policy, procedures addressing maintenance personnel, procedures addressing personnel security, procedures addressing physical access authorizations, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to ensure the cleared foreign nationals identified in MA-5(4).1.1.1 are used to conduct maintenance and diagnostic activities on the information system under the operational conditions identified in MA-5(4).1.1.1. |
| **MA-5(4).1.1.3** | **Examine** security clearances (or personnel screening records as appropriate) and an agreed-upon [*basic*] sample of maintenance records for an agreed-upon [*basic*] sample of personnel identified in MA-5(4).1.1.1 as conducting maintenance on the information system; [*reviewing*] for evidence that the measures identified in MA-5(4).1.1.2 are being applied. |
| **MA-5(4).1.1.4** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with information system maintenance responsibilities, organizational personnel with personnel security responsibilities, and/or organizational personnel with physical access control responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in MA-5(4).1.1.2 are being applied. |
|  |  |
| **MA-5(4).1.2.1** | **Examine** information system documentation; [*reviewing*] for Memorandums of Agreement between the organization and an agreed-upon [*basic*] sample of foreign nationals identified in MA-5(4).1.1.1. |
| **MA-5(4).1.2.2** | **Examine** Memorandums of Agreement identified in MA-5(4).1.2.1; [*reviewing*] for the approvals, consents, and detailed operational conditions under which foreign nationals are allowed to conduct maintenance and diagnostic activities on the information system. |