| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **IA-3** | DEVICE IDENTIFICATION AND AUTHENTICATION | |
| **IA-3.1**  **IA-3.1.1**  **IA-3.1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the specific and/or types of devices for which identification and authentication is required before establishing a connection to the information system; and* 2. *the information system uniquely identifies and authenticates the organization-defined devices before establishing a connection to the information system.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Identification and authentication policy; procedures addressing device identification and authentication; information system design documentation; list of devices requiring unique identification and authentication; device connection reports; information system configuration settings and associated documentation; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing device identification and authentication]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AC-2, AC-3, AC-4, AC-14  concurrent controls: AC-17, AC-18, AC-19, CA-3, CM-6, IA-2, IA-4, IA-5, IA-6, IA-7, MA-4  successor controls: IA-8 |
| **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. |
| **IA-3.1.1.1** | | **Examine** identification and authentication policy, procedures addressing device identification and authentication, security plan, or other relevant documents; [*reviewing*] for the specific and/or types of devices for which identification and authentication is required before establishing a connection to the information system. |
|  | |  |
| **IA-3.1.2.1** | | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to uniquely identify and authenticate the devices identified in IA-3.1.1.1 before establishing a connection to the information system. |
| **IA-3.1.2.2** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in IA-3.1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in IA-3.1.2.1. |
| **IA-3.1.2.3** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in IA-3.1.2.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 1** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **IA-3(1)** | DEVICE IDENTIFICATION AND AUTHENTICATION |
| **IA-3(1).1**  **IA-3(1).1.1**  **IA-3(1).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the information system authenticates devices before establishing remote network connections using bi-directional authentication between devices that is cryptographically based; and* 2. *the information system authenticates devices before establishing wireless network connections using bi-directional authentication between devices that is cryptographically based.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Identification and authentication policy; procedures addressing device identification and authentication; information system design documentation; device connection reports; information system configuration settings and associated documentation; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing device identification and authentication]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AC-2, AC-3, AC-4, AC-14  concurrent controls: AC-17, AC-18, AC-19, CM-6, IA-2, IA-4, IA-5, IA-6. IA-7, SC-13  successor controls: IA-8 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **IA-3(1).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 authenticate devices before establishing remote network connections using bi-directional authentication between devices that is cryptographically based. |
| **IA-3(1).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in IA-3(1).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in IA-3(1).1.1.1. |
| **IA-3(1).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in IA-3(1).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  |  |
| **IA-3(1).1.2.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to authenticate devices before establishing wireless network connections using bi-directional authentication between devices that is cryptographically based. |
| **IA-3(1).1.2.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in IA-3(1).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in IA-3(1).1.2.1. |
| **IA-3(1).1.2.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in IA-3(1).1.2.1; 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)** | |
| **IA-3(2)** | DEVICE IDENTIFICATION AND AUTHENTICATION |
| **IA-3(2).1**  **IA-3(2).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system authenticates devices before establishing network connections using bidirectional authentication between devices that is cryptographically based.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Identification and authentication policy; procedures addressing device identification and authentication; information system design documentation; device connection reports; information system configuration settings and associated documentation; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing device identification and authentication]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AC-2, AC-3, AC-4, AC-14  concurrent controls: AC-17, AC-18, AC-19, CM-6, IA-2, IA-4, IA-5, IA-6, IA-7, SC-13  successor controls: IA-8 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **IA-3(2).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 authenticate devices before establishing network connections using bidirectional authentication between devices that is cryptographically based. |
| **IA-3(2).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in IA-3(2).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in IA-3(2).1.1.1. |
| **IA-3(2).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in IA-3(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)** | |
| **IA-3(3)** | DEVICE IDENTIFICATION AND AUTHENTICATION |
| **IA-3(3).1**  **IA-3(3).1.1**  **IA-3(3).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization standardizes, with regard to dynamic address allocation, Dynamic Host Control Protocol (DHCP) lease information and the time assigned to DHCP-enabled devices; and* 2. *the organization audits DHCP lease information (including IP addresses) when assigned to a DHCP-enabled devices.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Identification and authentication policy; procedures addressing device identification and authentication; information system design documentation; information system configuration settings and associated documentation; DHCP lease information; device connection reports; other relevant documents or records]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AU-2, AU-3, AU-6, AU-7, AU-8, AU-12, CM-6, IA-4, IA-5, SC-7, SI-4  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **IA-3(3).1.1.1** | **Examine** identification and authentication policy, procedures addressing device identification and authentication, 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 standardize DHCP lease information and the time assigned to DHCP-enabled devices. |
| **IA-3(3).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in IA-3(3).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in IA-3(3).1.1.1. |
| **IA-3(3).1.1.3** | **Examine** DHCP lease information for an agreed-upon [*basic*] sample of DHCP-enabled devices listed in device connection reports; [*reviewing*] for evidence that the measures identified in IA-3(3).1.1.1 are being applied. |
| **IA-3(3).1.1.4** | **Interview** an agreed-upon [*basic*] sample of organizational personnel responsible for standardizing DHCP lease information; conducting [*basic*] discussions for further evidence that the measures identified in IA-3(3).1.1.1 are being applied. |
| **IA-3(3).1.1.5** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in IA-3(3).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  |  |
| **IA-3(3).1.2.1** | **Examine** identification and authentication policy, procedures addressing device identification and authentication, security plan, or other relevant documents; [*reviewing*] for the measures (including automated mechanisms and their configuration settings) to be employed to audit DHCP lease information (including IP addresses) when assigned to DHCP-enabled devices. |
| **IA-3(3).1.2.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in IA-3(3).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in IA-3(3).1.2.1. |
| **IA-3(3).1.2.3** | **Examine** audit records for an agreed-upon [*basic*]sample of DHCP-enabled devices listed in device connection reports; [*reviewing*] for evidence that the measures identified in IA-3(3).1.2.1 are being applied. |
| **IA-3(3).1.2.4** | **Interview** an agreed-upon [*basic*] sample of organizational personnel responsible for auditing DHCP lease information; conducting [*basic*] discussions for further evidence that the measures identified in IA-3(3).1.2.1 are being applied. |
| **IA-3(3).1.2.5** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in IA-3(3).1.2.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |