| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **SC-11** | TRUSTED PATH | |
| **SC-11.1**  **SC-11.1.1**  **SC-11.1.2**  **SC-11.1.3** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the security functions within the information system to be included in a trusted communications path;* 2. *the organization-defined security functions include information system authentication and reauthentication; and* 3. *the information system establishes a trusted communications path between the user and the organization-defined security functions within the information system.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing trusted communications paths; security plan; information system design documentation; information system configuration settings and associated documentation; assessment results from independent, testing organizations; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing trusted communications paths within the information system]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-4, AC-6, AC-11, AC-16, CM-6, IA-2  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-11.1.1.1** | | **Examine** system and communications protection policy, procedures addressing trusted communications paths, security plan, or other relevant documents; [*reviewing*] for the security functions within the information system to be included in a trusted communications path. |
|  | |  |
| **SC-11.1.2.1** | | **Examine** the security functions identified in SC-11.1.1.1; [*reviewing*] for information system authentication and re-authentication functions. |
|  | |  |
| **SC-11.1.3.1** | | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to establish a trusted communications path between the user and the security functions identified in SC-11.1.1.1. |
| **SC-11.1.3.2** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SC-11.1.3.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-11.1.3.1. |
| **SC-11.1.3.3** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-11.1.3.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | | |