| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 2 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **AC-8** | SYSTEM USE NOTIFICATION | |
| **AC-8.1**  **AC-8.1.1**  **AC-8.1.2**  **AC-8.1.2a**  **AC-8.1.2b**  **AC-8.1.2c**  **AC-8.1.2d**  **AC-8.1.3** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization approves the information system use notification message or banner to be displayed by the information system before granting access to the system;* 2. *the information system displays the approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that:*    * *users are accessing a U.S. Government information system;*    * *system usage may be monitored, recorded, and subject to audit;*    * *unauthorized use of the system is prohibited and subject to criminal and civil penalties; and*    * *use of the system indicates consent to monitoring and recording; and* 3. *the information system retains the notification message or banner on the screen until the user takes explicit actions to log on to or further access the information system.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; privacy and security policies; procedures addressing system use notification; documented approval of information system use notification messages or banners; information system notification messages; information system configuration settings and associated documentation; information system audit records for user acceptance of notification message or banner; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing the access control policy for system use notification]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6, PL-4, PS-6, 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. |
| **AC-8.1.1.1** | | **Examine** access control policy, privacy and security policy, procedures addressing system use notification, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to approve the information use notification message or banner to be displayed by the information system before granting access to the system. |
| **AC-8.1.1.2** | | **Examine** documented approval of information system use notification message or banner displayed by the information system before granting access to the system; [*reviewing*] for evidence that the measures identified in AC-8.1.1.1 are being applied. |
|  | |  |
| **AC-8.1.2.1** | | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to display the approved system use notification message or banner before granting access to the system. |
| **AC-8.1.2.2** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-8.1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-8.1.2.1. |
| **AC-8.1.2.3** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-8.1.2.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
| **AC-8.1.2.4** | | **Examine** access control policy, privacy and security policy, procedures addressing system use notification, security plan, or other relevant documents; [*reviewing*] for the applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance that establish the appropriate privacy and security notices to be provided when the information system displays an approved system use notification message or banner before granting access to the system. |
| **AC-8.1.2.5**  **AC-8.1.2.5.a**  **AC-8.1.2.5.b**  **AC-8.1.2.5.c**  **AC-8.1.2.5.d** | | **Examine** information system use notification message or banner; [*reviewing*] for evidence that the system use notification message or banner provides privacy and security notices consistent with the applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance identified in AC-8.1.2.4, and states that:   * + users are accessing a U.S. Government information system;   + system usage may be monitored, recorded, and subject to audit;   + unauthorized use of the system is prohibited and subject to criminal and civil penalties; and   + use of the system indicates consent to monitoring and recording. |
|  | |  |
| **AC-8.1.3.1** | | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to retain the notification message or banner on the screen until the user takes explicit actions to log on to or further access the information system. |
| **AC-8.1.3.2** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-8.1.3.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-8.1.3.1. |
| **AC-8.1.3.3** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-8.1.3.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |

|  |  |  |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 2 of 2 | | |
| **AC-8.2**  **AC-8.2.1**  **AC-8.2.2**  **AC-8.2.3** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the information system (for publicly accessible systems) displays the system use information when appropriate, before granting further access;* 2. *the information system (for publicly accessible systems) displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and* 3. *the information system (for publicly accessible systems) includes in the notice given to public users of the information system, a description of the authorized uses of the information system.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; privacy and security policies; procedures addressing system use notification; documented approval of information system use notification messages or banners; information system notification messages; information system configuration settings and associated documentation; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing the access control policy for system use notification]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6, PL-4, PS-6, 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\*\*** |
| **AC-8.2.1.1** | | **Examine** access control policy, privacy and security policy, procedures addressing system use notification, security plan, or other relevant documents; [*reviewing*] for when displaying the system use information is considered appropriate for publicly accessible systems, before granting further access. |
| **AC-8.2.1.2** | | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to display the system use information for publicly accessible systems, when considered appropriate as identified in AC-8.2.1.1. |
| **AC-8.2.1.3** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-8.2.1.2; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-8.2.1.2. |
| **AC-8.2.1.4** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-8.2.1.2; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |  |
| **AC-8.2.2.1** | | **Examine** information system notification messages for publicly accessible systems; [*reviewing*] for references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities. |
|  | |  |
| **AC-8.2.3.1** | | **Examine** information system notification messages for publicly accessible systems; [*reviewing*] for a description of the authorized uses of the information system. |
|  | | |