For High-Impact Information Systems

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

AC-1 ACCESS CONTROL POLICY AND PROCEDURES – The organization develops, disseminates, and periodically reviews/ updates: (i) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.

AC-1.1 – Examine access control policy and procedures and other relevant documents or records to determine if the following requirements are met **and**

Interview organizational personnel with access control responsibilities.

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization develops and documents access control policy and procedures.				
(ii)	The organization disseminates access control policy and procedures to appropriate elements within the organization.				
(iii)	Responsible parties within the organization periodically review access control policy and procedures.				
(iv)	The organization updates access control policy and procedures when organizational review indicates that updates are required.				

AC-1.2 – **Examine** access control policy and procedures and other relevant documents or records to determine if the following requirements are met **and**

Interview organizational personnel with access control responsibilities.

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Access control policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among				

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
	organizational entities, and compliance.				
(ii)	The access control policy is consistent with the organization's mission and functions and applicable laws, directives, policies, regulations, standards, and guidance.				
(iii)	The access control procedures address all areas identified in the access control policy and address achieving policy-compliant implementations of all associated security controls.				

AC-2 ACCOUNT MANAGEMENT – The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts [*Assignment: organization-defined frequency, at least annually*].

AC-2.1 – **Examine** access control policy; account management procedures; information system security plan (for organization-defined account review frequency); list of active user and system accounts; list of recently separated or terminated employees; list of recently disabled information system accounts; system-generated records with user IDs and last login date; other relevant documents or records, **and**

Interview organizational personnel with account management responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts;				
(ii)	The organization defines the frequency of information system account reviews;				
(iii)	The organization reviews information system accounts at the organization-defined frequency, at least annually; and				
(iv)	The organization initiates required actions on information system accounts based on the review.				

AC-2(1) Account Management - The organization employs automated mechanisms to support the management of information system accounts.

AC-2(1).1 - Examine Access control policy; account management procedures; information system design documentation, information system configuration settings and associated documentation; list of account management functions; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization employs automated mechanisms to support information system account management functions. i				

and

Test: Automated mechanisms implementing account management functions.

Test Steps		S	N	Findings	Initials & Date
1					

AC-2(2) Account Management - The information system automatically terminates temporary and emergency accounts after [Assignment: organization-defined time period for each type of account].

AC-2(2).1 – Examine - Access control policy; account management procedures; information system security plan (for organization-defined time period for automatic account termination by account type); information system design documentation, information system configuration settings and associated documentation; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization defines a time period after which the information system terminates temporary and emergency accounts.				
(ii)	The information system automatically terminates temporary and emergency accounts after organization-defined time period for each type of account.				

and

Test: Automated mechanisms implementing account management functions.

	Test Steps	S	N	Findings	Initials & Date
1					

AC-2(3) Account Management - The information system automatically disables inactive accounts after [Assignment: organization-defined time period].

AC-2(3).1 – Examine - Access control policy; account management procedures; information system security plan (for organization-defined time period for automatic account disabling); information system design documentation; information system configuration settings and associated documentation; information system-generated list of last login dates; information system-generated list of active accounts; other relevant documents or records. to determine if the following requirements are met:

	Requirement	S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization defines a time period after which the information system disables inactive accounts.				
(ii)	The information system automatically disables inactive accounts after organization-defined time period.				

and

Test: Automated mechanisms implementing account management functions.

	Test Steps	S	N	Findings	Initials & Date
1					

AC-2(4) Account Management - The organization employs automated mechanisms to audit account creation, modification, disabling, and termination actions and to notify, as required, appropriate individuals.

AC-2(4).1 – Examine - Access control policy; account management procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the organization employs automated mechanisms to audit account creation, modification, disabling, and termination actions and to notify, as required, appropriate individuals.				

and

Test: Automated mechanisms implementing account management functions.

Test Steps		S	N	Findings	Initials & Date
1					

AC-3 ACCESS ENFORCEMENT – The information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy.

AC-3.1 – Examine access enforcement policy and procedures; information system configuration settings and associated documentation; list of assigned authorizations (user privileges); information system audit records; other relevant documents or records to determine if the following requirements are met

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy.				
(ii)	User privileges on the information system are consistent with the documented user authorizations				

and

Test: Automated mechanisms implementing access enforcement policy.

Test Steps	S	N	Findings	Initials & Date

Test Steps		S	N	Findings	Initials & Date
1					

AC-3(1).1 – Examine access enforcement policy and procedures; list of privileged functions and security relevant information; information system configuration settings and associated documentation; list of assigned authorizations (user privileges); information system audit records; other relevant documents or records to determine if the following requirements are met **and**

Test: Automated mechanisms implementing access enforcement policy.

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization explicitly defines privileged functions and security-related information for the information system;				
(ii)	The organization explicitly authorizes personnel access to privileged functions and security-relevant information in accordance with organizational policy; and				
(iii)	The information system restricts access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel, such as security administrators.				

AC-4 INFORMATION FLOW ENFORCEMENT – The information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.

AC-4.1 – Examine Access control policy; procedures addressing information flow enforcement; information system design documentation; information system configuration settings and associated documentation; information system baseline configuration; list of information flow authorizations; information system audit records; other relevant documents or records.

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.				

and

Test: Automated mechanisms implementing information flow enforcement policy.

	Test Steps	S	N	Findings	Initials & Date
1					

AC-4.2 – Examine Access control policy; procedures addressing information flow enforcement; information system interconnection agreements; information system configuration settings and associated documentation; list of information flow control authorizations; information system audit records; other relevant documents or records.

	Requirement	S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if interconnection agreements address the types of permissible and impermissible flow of information between information systems and the required level of authorization to allow information flow as defined in the information flow enforcement policy and procedures.				

AC-5 SEPARATION OF DUTIES – The information system enforces separation of duties through assigned access authorizations.

AC-5.1 – **Examine** separation of duties policy and procedures; information system configuration settings and associated documentation; list of separation of duties authorizations; information system audit records; other relevant documents

and

Interview organizational personnel with responsibilities for defining appropriate divisions of responsibility and separation of duties to determine if the following requirements are met:

.

	Requirement	S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals.				

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(ii)	The information system enforces separation of duties through assigned access authorizations.				

and

Test: Automated mechanisms implementing separation of duties policy.

Test Steps		S	N	Findings	Initials & Date
1					

AC-6 LEAST PRIVILEGE – The information system enforces the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.

AC-6.1 – **Examine** access control policy; procedures addressing least privilege; list of assigned access authorizations (user privileges); information system configuration settings and associated documentation; information system audit records; other relevant documents or records **and**

Interview organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks.

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization assigns the most restrictive set of rights/privileges or accesses needed by users for the performance of specified tasks.				
(ii)	The information system enforces the most restrictive set of rights/privileges or accesses needed by users.				

AC-7 UNSUCCESSFUL LOGIN ATTEMPTS – The information system enforces a limit of [*Assignment: organization-defined number*] consecutive invalid access attempts by a user during a [*Assignment: organization-defined time period*] time period. The information system automatically [*Selection: locks the account/node for an* [*Assignment: organization-defined time period*], *delays next login prompt according to* [*Assignment: organization-defined delay algorithm.*]] when the maximum number of unsuccessful attempts is exceeded.

AC-7.1 – Examine access control policy; procedures addressing unsuccessful logon attempts; information system security plan (for organization-defined maximum number of invalid access attempts within organization-defined time period, automatic response when maximum number of invalid access attempts is exceeded, time period for lock out mode or delay period); information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization defines the maximum number of consecutive invalid access attempts to the information system by a user and the time period in which the consecutive invalid access attempts occur;				
(ii)	The information system enforces the organization-defined limit of consecutive invalid access attempts by a user during the organization-defined time period;				
(iii)	The organization defines the time period for lock out mode or delay period;				
(iv)	The organization selects either a lock-out mode for the organization-defined period or delays next login prompt for the organization-defined delay period for information system responses to consecutive invalid access attempts; and				
(v)	The information system enforces the organization-selected lock-out mode or delayed login prompt.				

and

Test automated mechanisms implementing the access control policy for unsuccessful login attempts.

Test Steps		S	N	Findings	Initials & Date
1					

AC-8 SYSTEM USE NOTIFICATION – The information system displays an approved, system use notification message before granting system access informing potential users: (i) that the user is accessing a U.S. Government information system; (ii) that system usage may be monitored, recorded, and subject to audit; (iii) that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) that use of the system indicates consent to monitoring and recording. The system use notification message

provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on to the information system.

AC-8.1- Examine access control policy; procedures addressing system use notification; information system notification messages; information system configuration settings and associated documentation; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The information system displays a system use notification message before granting system access informing potential users of the following: • The user is accessing a US government information system; • System usage may be monitored, recorded, and subject to audit; • Unauthorized system use is prohibited and subject to criminal and civil penalties; and • System use indicates consent to `monitoring and recording.				
(ii)	The system-use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries).				
(iii)	The organization approves the information system use notification message before its use.				
(iv)	The system-use notification message remains on the screen until the user takes explicit actions to log on to the information system.				

and

Test automated mechanisms implementing the access control policy for system use notification.

Test Steps		S	N	Findings	Initials & Date
1					

AC-9 PREVIOUS LOGON NOTIFICATION – The information system notifies the user, upon successful logon, of the date and time of the last logon, and the number of unsuccessful logon attempts since the last successful logon.

AC-9.1 - **Examine** access control policy; procedures addressing previous logon notification; information system notification messages; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records to determine if the following requirement is met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The information system, upon successful logon, displays the date and time of the last logon and the number of unsuccessful logon attempts since the last successful logon.				

and

Test automated mechanisms implementing the access control policy for previous logon notification to determine if the same requirement is met.

Test Steps		S	N	Findings	Initials & Date
1	Verify that the access control settings are in compliance with the agency's security hardening guide.				

AC-10 CONCURRENT SESSION CONTROL – The information system limits the number of concurrent sessions for any user to [*Assignment: organization-defined number of sessions*].

AC-10.1 - **Examine** access control policy; procedures addressing concurrent session control; information system configuration settings and associated documentation; information system security plan (for organization-defined limit for concurrent sessions for information system users); other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization defines the maximum number of concurrent sessions for information system users; and				

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(ii)	The information system limits the number of concurrent sessions for users to the organization-defined number of sessions.				

and

Test automated mechanisms implementing the access control policy for concurrent session control.

Test Steps		S	N	Findings	Initials & Date
1	Verify that the access control settings are in compliance with the agency's security hardening guide.				

AC-11 SESSION LOCK - The information system prevents further access to the system by initiating a session lock after [*Assignment: organization-defined time period*] of inactivity, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures.

AC-11.1 - Examine access control policy; procedures addressing session lock; information system design documentation; information system configuration settings and associated documentation; information system security plan (for organization-defined time period for user inactivity after which automatic session lock is to be activated); other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization defines the time period of user inactivity that initiates a session lock within the information system;				
(ii)	The information system initiates a session lock after the organization-defined time period of inactivity; and				
(iii)	The information system maintains the session lock until the user reestablishes access using appropriate identification and authentication procedures.				

and

Test automated mechanisms implementing the access control policy for session lock.

Test Steps		S	N	Findings	Initials & Date
1					

AC-12 SESSION TERMINATION - The information system automatically terminates a remote session after [*Assignment: organization-defined time period*] of inactivity.

AC-12.1 - Examine access control policy; procedures addressing session termination; information system design documentation; information system configuration settings and associated documentation; information system security plan (for organization-defined time period for user inactivity after which automatic session termination is to be activated); other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization defines the time period of user inactivity that initiates a remote session termination within the information system; and				
(ii)	The information system automatically terminates a remote session after the organization-defined time period of inactivity.				

and

Test automated mechanisms implementing the access control policy for session termination.

Test Steps		S	N	Findings	Initials & Date
1					

AC-12(1).1 - **Examine** access control policy; procedures addressing supervision and review of access control enforcement and usage; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records to determine if the same requirement is met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if automatic session termination applies to local and remote sessions.				

and

Test automated mechanisms implementing the access control policy for session termination.

Test Steps		S	N	Findings	Initials & Date
1					

AC-13 SUPERVISION AND REVIEW - ACCESS CONTROL - The organization supervises and reviews the activities of users with respect to the enforcement and usage of information system access controls.

AC-13.1 - Examine access control policy; procedures addressing supervision and review of access control enforcement and usage; organizational records of supervisory notices of disciplinary actions to users; information system exception reports; other relevant documents or records **and**

Interview organizational personnel with supervisory and access control responsibilities.

.

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the organization supervises and reviews the activities of users with respect to the enforcement and usage of information system access controls.				

AC-13(1).1 - **Examine** access control policy; procedures addressing supervision and review of access control enforcement and usage; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records to determine if the same requirement is met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the organization employs automated mechanisms within the information system to support and facilitate the review of user activities.				

and

Test automated mechanisms supporting the access control policy for supervision and review of user activities.

Test Steps		S	N	Findings	Initials & Date
1					

AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION - The organization identifies and documents specific user actions that can be performed on the information system without identification or authentication.

AC-14.1- Examine access control policy; procedures addressing permitted actions without identification and authentication; information system configuration settings and associated documentation; information system security plan; other relevant documents or records to determine if the same requirement is met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the organization identifies and documents specific user actions that can be performed on the information system without identification or authentication.				

and

Test automated mechanisms implementing the access control policy for permitted actions without identification and authentication.

Test Steps		S	N	Findings	Initials & Date
1					

AC-14(1).1 - Examine access control policy; procedures addressing permitted actions without identification and authentication; information system configuration settings and associated documentation; list of organization-defined actions that can be performed without identification and authentication; other relevant documents or records **and**

Interview organizational personnel with responsibilities for defining permitted actions without identification and authentication to determine if the same requirement is met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission objectives.				

AC-15 ACCESS CONTROL - The information system marks output using standard naming conventions to identify any special dissemination, handling, or distribution instructions

AC-15.1 - Examine access control policy; procedures for addressing automated marking of information system output; information system output; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records **and**

Interview organizational personnel with responsibilities for defining special dissemination, handling, and marking instructions for information system output to determine if the same requirement is met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization identifies standard naming conventions for information system output.				
(ii)	The information system marks output using standard naming conventions to identify any special dissemination, handling, or distribution instructions.				

and

Test automated mechanisms implementing automated marking of information system output.

Test Steps	S	N	Findings	Initials & Date

Test Steps		S	N	Findings	Initials & Date
1					

AC-17 REMOTE ACCESS - The organization authorizes, monitors, and controls all methods of remote access to the information system.

AC-17.1 - Examine access control policy; procedures addressing remote access to the information system; list of information system accounts; information system configuration settings and associated documentation; information system audit records; other relevant documents or records, **and**

Interview organizational personnel with remote access authorization, monitoring, and control responsibilities to determine if the same requirement is met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the organization documents, monitors, and controls all methods of remote access to the information system.				

AC-17(1).1 - Examine access control policy; procedures addressing remote access to the information system; list of information system accounts; information system configuration settings and associated documentation; other relevant documents or records to determine if the same requirement is met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the organization documents, monitors, and controls all methods of remote access to the information system.				

and

Test automated mechanisms implementing the access control policy for remote access.

Test Steps		S	N	Findings	Initials & Date
1					

AC-17(2).1 - Examine access control policy; procedures addressing remote access to the information system; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records to determine if the same requirement is met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the information system employs cryptography to protect the confidentiality and integrity of remote access sessions.				

and

Test automated mechanisms implementing cryptographic protections for remote access.

Test Steps		S	N	Findings	Initials & Date
1					

AC-17(3).1 - Examine access control policy; procedures addressing remote access to the information system; information system design documentation; list of managed access control points; information system configuration settings and associated documentation; list of information system accounts; information system audit records; other relevant documents or records to determine if the same requirement is met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization defines managed access control points for remote access to the information system; and				
(ii)	The information system controls all remote accesses through a limited number of managed access control points.				

and

Test automated mechanisms implementing the access control policy for remote access.

	Test Steps	S	N	Findings	Initials & Date
1					

17(4).1 - Examine access control policy; procedures addressing remote access to the information system; list of information system accounts; information system configuration settings and associated documentation; information system security plan; information system audit records; other relevant documents or records to determine if the same requirement is met:

	Requirement	S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization defines the situations and compelling operational needs when remote access to privileged functions on the information system is allowed; and				
(ii)	The organization permits remote access for privileged functions only for compelling operational needs and documents the rationale for such access in the security plan for the information system.				

and

Test automated mechanisms implementing the access control policy for remote access.

	Test Steps	S	N	Findings	Initials & Date
1					

AC-18 WIRELESS ACCESS RESTRICTIONS - The organization: (i) establishes usage restrictions and implementation guidance for wireless technologies; and (ii) authorizes, monitors, controls wireless access to the information system.

AC-18.1 - Examine access control policy; procedures addressing wireless implementation and usage (including restrictions); NIST Special Publications 800-48 and 800-97; activities related to wireless authorization, monitoring, and control; information system audit records; other relevant documents or records to determine if the same requirement is met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization establishes usage restrictions and implementation guidance for wireless technologies;				
(ii)	The organization authorizes, monitors, and controls wireless access to the information system; and				
(iii)	The wireless access restrictions are consistent with NIST Special Publications 800-48 and 800-97.				

and

Test wireless access usage and restrictions to determine if the same requirement is met:

Test Steps		S	N	Findings	Initials & Date
1	Attempt to log on to wireless access point.				

AC-18(1).1 - Examine access control policy; procedures addressing wireless implementation and usage (including restrictions); information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine if the same requirement is met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the organization uses authentication and encryption to protect wireless access to the information system.				

and

Test automated mechanisms implementing wireless access to the information system.

Test Steps		S	N	Findings	Initials & Date
1					

AC-18(2).1 - Examine access control policy; procedures addressing wireless implementation and usage (including restrictions); information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine if the same requirement is met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the defines the frequency of scans for unauthorized wireless access points;				
(ii)	The organization scans for unauthorized wireless access points in accordance with organization-defined frequency and takes appropriate action if such an access point are discovered.				

and

Test scanning procedure for unauthorized wireless access points.

Test Steps		S	N	Findings	Initials & Date
1					

AC-19 ACCESS CONTROL FOR PORTABLE AND MOBILE DEVICES - The organization: (i) establishes usage restrictions and implementation guidance for organization-controlled portable and mobile devices; and (ii) authorizes, monitors, and controls device access to organizational information systems.

AC-19.1 - Examine access control policy; procedures addressing access control for portable and mobile devices; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records, **and**

Interview (DEPTH, COVERAGE): Organizational personnel who use portable and mobile devices to access the information system to determine if the same requirement is met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization defines a mandatory suite of protective software and security protocols to be installed on and executed by the information system and portable and mobile devices;				
(ii)	The organization establishes usage restrictions and implementation guidance for organization-controlled portable and mobile devices; and				
(iii)	The organization authorizes, monitors, and controls device access to organizational information systems.				

and

Test automated mechanisms implementing access control policy for portable and mobile devices.

Test Steps		S	N	Findings	Initials & Date
1					

AC-20 USE OF EXTERNAL INFORMATION SYSTEMS - The organization establishes terms and conditions for authorized individuals to: (i) access the information system from an external information system; and (ii) process, store, and/or transmit organization-controlled information using an external information system.

AC-20.1 - Examine access control policy; procedures addressing the use of external information systems; external information systems terms and conditions; list of types of applications accessible from external information systems; maximum FIPS 199 impact level for information processed, stored, or transmitted on external information systems; information system configuration settings and associated documentation; other relevant documents or records, **and**

Interview organizational personnel who use external information systems to access the information system to determine if the same requirement is met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization defines the types of applications that can be				

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
	accessed from the external information system;				
(ii)	The organization defines the maximum FIPS 199 security category of information that can be processed, stored, and transmitted on the external information system; and				
(iii)	The organization establishes terms and conditions for authorized individuals to access the information system from an external information system that include the types of applications that can be accessed on the organizational information system from the external information system and the maximum FIPS 199 security category of information that can be processed, stored, and transmitted on the external information system.				

AC-20(1).1 - Examine access control policy; procedures addressing the use of external information systems; information system security plan; information system configuration settings and associated documentation; information system connection or processing agreements; account management documents; list of information system accounts; other relevant documents or records to determine if the same requirement is met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization verifies, for authorized exceptions, the employment of required security controls on the external system as specified in the organization's information security policy and system security plan when allowing connections to the external information system.				
(ii)	The organization approves, for authorized exceptions, information system connection or processing agreements with the organizational entity hosting the external information system.				