

Department of the Interior
Security Control Standard
Access Control

July 2011

Version: 1.3



Signature Approval Page

Designated Official	
Bernard J. Mazer, Department of the Interior, Chief Information Officer	
Signature:	Date:

REVISION HISTORY

Author	Version	Revision Date	Revision Summary
Chris Peterson	0.1	November 30, 2010	Initial draft
Timothy Brown	0.2	December 02, 2010	Incorporated comments into body text
Timothy Brown	0.21	January 07, 2011	Added introductory paragraph
Timothy Brown	0.22	February 15, 2011	Added cloud controls to “high”
Chris Peterson	1.0	February 17, 2011	Final review of controls; remove margin notes
Lawrence K. Ruffin	1.1	April 29, 2011	Final revisions and version change to 1.1
Lawrence K. Ruffin	1.2	May 5, 2011	Incorporated language under AC-20 addressing use of GFE vs non-GFE
Lawrence K. Ruffin	1.3	July 26, 2011	Modified language in AC-20 to eliminate specific reference to WPA2(AES) and instead refer to applicable NIST standards; and modified AC-8 to incorporate the DOI approved content for system use notification messages or banners

TABLE OF CONTENTS

REVISION HISTORY	3
TABLE OF CONTENTS	4
SECURITY CONTROL STANDARD: ACCESS CONTROL	5
AC-1 ACCESS CONTROL POLICY AND PROCEDURES	5
AC-2 ACCOUNT MANAGEMENT	6
AC-3 ACCESS ENFORCEMENT	7
AC-4 INFORMATION FLOW ENFORCEMENT	8
AC-5 SEPARATION OF DUTIES	9
AC-6 LEAST PRIVILEGE	9
AC-7 UNSUCCESSFUL LOGIN ATTEMPTS	10
AC-8 SYSTEM USE NOTIFICATION	11
AC-10 CONCURRENT SESSION CONTROL	12
AC-11 SESSION LOCK	13
AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION/AUTHENTICATION	13
AC-16 SECURITY ATTRIBUTES	14
AC-17 REMOTE ACCESS	14
AC-18 WIRELESS ACCESS	16
AC-19 ACCESS CONTROL FOR MOBILE DEVICES	17
AC-20 USE OF EXTERNAL INFORMATION SYSTEMS	18
AC-22 PUBLICLY ACCESSIBLE CONTENT	21

SECURITY CONTROL STANDARD: ACCESS CONTROL

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 describes the required process for selecting and specifying security controls for an information system based on its security categorizing, including tailoring the initial set of baseline security controls and supplementing the tailored baseline as necessary based on an organizational assessment of risk.

This standard specifies organization-defined parameters that are deemed necessary or appropriate to achieve a consistent security posture across the Department of the Interior. In addition to the NIST SP 800-53 Access Control (AC) control family standard, supplemental information is included that establishes an enterprise-wide standard for specific controls within the control family. In some cases additional agency-specific or Office of Management and Budget (OMB) requirements have been incorporated into relevant controls. Where the NIST SP 800-53 indicates the need for organization-defined parameters or selection of operations that are not specified in this supplemental standard, the System Owner shall appropriately define and document the parameters based on the individual requirements, purpose, and function of the information system. The supplemental information provided in this standard is required to be applied when the Authorizing Official (AO) has selected the control, or control enhancement, in a manner that is consistent with the Department's IT security policy and associated information security Risk Management Framework (RMF) strategy.

Additionally, information systems implemented within cloud computing environments shall select, implement, and comply with any additional and/or more stringent security control requirements as specified and approved by the Federal Risk and Authorization Management Program (FedRAMP) unless otherwise approved for risk acceptance by the AO. The additional controls required for implementation within cloud computing environments are readily identified within the Priority and Baseline Allocation table following each control and distinguished by the control or control enhancement represented in **bold red text**.

AC-1 ACCESS CONTROL POLICY AND PROCEDURES

Applicability: All Information Systems

Control: The organization develops, disseminates, and reviews/updates annually:

- a) A formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
- b) Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the access control family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The access control policy can be included as part of the general information security policy for the organization. Access control procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the access control policy. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	LOW AC-1	MOD AC-1	HIGH AC-1
-----------	-----------------	-----------------	------------------

AC-2 ACCOUNT MANAGEMENT

Applicability: All Information Systems

Control: The organization manages information system accounts, including:

- a) Identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary);
- b) Establishing conditions for group membership;
- c) Identifying authorized users of the information system and specifying access privileges;
- d) Requiring appropriate approvals for requests to establish accounts;
- e) Establishing, activating, modifying, disabling, and removing accounts;
- f) Specifically authorizing and monitoring the use of guest/anonymous and temporary accounts;
- g) Notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes;
- h) Deactivating: (i) temporary accounts that are no longer required; and (ii) accounts of terminated or transferred users;
- i) Granting access to the system based on: (i) a valid access authorization; (ii) intended system usage; and (iii) other attributes as required by the organization or associated missions/business functions; and
- j) Reviewing accounts annually.

Supplemental Guidance: The identification of authorized users of the information system and the specification of access privileges is consistent with the requirements in other security controls in the security plan. Users requiring administrative privileges on information system accounts receive additional scrutiny by organizational officials responsible for approving such accounts and privileged access. Related controls: AC-3, AC-4, AC-5, AC-6, AC-10, AC-17, AC-19, AC-20, AU-9, IA-4, IA-5, CM-5, CM-6, MA-3, MA-4, MA-5, SA-7, SC-13, SI-9.

Control Enhancements:

1. The organization employs automated mechanisms to support the management of information system accounts.
2. The information system automatically terminates temporary and emergency accounts after 90 days.
3. The information system automatically disables inactive accounts after 90 days.
4. The information system automatically audits account creation, modification, disabling, and termination actions and notifies, as required, appropriate individuals.

7. The organization:
 1. Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes information system and network privileges into roles; and
 2. Tracks and monitors privileged role assignments.

Enhancement Supplemental Guidance: Privileged roles include, but are not limited to: key management, network and system administration, database administration, web administration.

References: None.

Priority and Baseline Allocation:

P1	LOW AC-2	MOD AC-2 (1) (2) (3) (4) (7)	HIGH AC-2 (1) (2) (3) (4) (7)
-----------	-----------------	-------------------------------------	--------------------------------------

AC-3 ACCESS ENFORCEMENT

Applicability: All Information Systems

Control: The information system enforces approved authorizations for logical access to the system in accordance with applicable policy.

Supplemental Guidance: Access control policies (e.g., identity-based policies, role-based policies, attribute-based policies) and access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) are employed by organizations to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system. In addition to enforcing authorized access at the information system level, access enforcement mechanisms are employed at the application level, when necessary, to provide increased information security for the organization. Consideration is given to the implementation of an audited, explicit override of automated mechanisms in the event of emergencies or other serious events. If encryption of stored information is employed as an access enforcement mechanism, the cryptography used is FIPS 140-2 (as amended) compliant. For classified information, the cryptography used is largely dependent on the classification level of the information and the clearances of the individuals having access to the information. Mechanisms implemented by AC-3 are configured to enforce authorizations determined by other security controls. Related controls: AC-2, AC-4, AC-5, AC-6, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AU-9, CM-5, CM-6, MA-3, MA-4, MA-5, SA-7, SC-13, SI-9.

Control Enhancements:

3. The information system enforces role-based access control over all users and resources where the policy rule set for each policy specifies:
 - a. Access control information (i.e., attributes) employed by the policy rule set (e.g., position, nationality, age, project, time of day); and
 - b. Required relationships among the access control information to permit access.

Enhancement Supplemental Guidance: Nondiscretionary access control policies that may be implemented by organizations include, for example, Attribute-Based Access Control, Mandatory Access Control, and Originator Controlled Access Control. Nondiscretionary access control policies may be employed by organizations in addition to the employment of discretionary access control policies.

For Mandatory Access Control (MAC): Policy establishes coverage over all subjects and objects under its control to ensure that each user receives only that information to which the user is authorized access based on classification of the information, and on user clearance and formal access authorization. The information system assigns appropriate security attributes (e.g., labels/security domains/types) to subjects and objects, and uses these attributes as the basis for MAC decisions. The Bell-LaPadula security model defines allowed access with regard to an organization-defined set of strictly hierarchical security levels as follows: A subject can read an object only if the security level of the subject dominates the security level of the object and a subject can write to an object only if two conditions are met: the security level of the object dominates the security level of the subject, and the security level of the user's clearance dominates the security level of the object (no read up, no write down).

For Role-Based Access Control (RBAC): Policy establishes coverage over all users and resources to ensure that access rights are grouped by role name, and access to resources is restricted to users who have been authorized to assume the associated role.

References: None.

Priority and Baseline Allocation:

P1	LOW AC-3	MOD AC-3 (3)	HIGH AC-3 (3)
-----------	-----------------	---------------------	----------------------

AC-4 INFORMATION FLOW ENFORCEMENT

Applicability: Moderate and High Impact Information Systems

Control: The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.

Supplemental Guidance: Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. A few examples of flow control restrictions include: keeping export controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization, and not passing any web requests to the Internet that are not from the internal web proxy. Information flow control policies and enforcement mechanisms are commonly employed by organizations to control the flow of information between designated sources and destinations (e.g., networks, individuals, devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Specific examples of flow control enforcement can be found in boundary protection devices (e.g., proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict information system services, provide a packet-filtering capability based on header information, or message-filtering capability based on content (e.g., using key word searches or document characteristics). Mechanisms implemented by AC-4 are configured to enforce authorizations determined by other security controls. Related controls: AC-17, AC-19, AC-21, CM-7, SA-8, SC-2, SC-5, SC-7, SC-18.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD AC-4	HIGH AC-4
-----------	-------------------------	-----------------	------------------

AC-5 SEPARATION OF DUTIES

Applicability: Moderate and High Impact Information Systems

Control: The organization:

- a. Separates duties of individuals as necessary, to prevent malevolent activity without collusion;
- b. Documents separation of duties; and
- c. Implements separation of duties through assigned information system access authorizations.

Supplemental Guidance: Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, configuration management, quality assurance and testing, network security); (iii) security personnel who administer access control functions do not administer audit functions; and (iv) different administrator accounts for different roles. Access authorizations defined in this control are implemented by control AC-3. Related controls: AC-3.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD AC-5	HIGH AC-5
-----------	-------------------------	-----------------	------------------

AC-6 LEAST PRIVILEGE

Applicability: Moderate and High Impact Information Systems

Control: The organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

Supplemental Guidance: The access authorizations defined in this control are largely implemented by control AC-3. The organization employs the concept of least privilege for specific duties and information systems (including specific ports, protocols, and services) in accordance with risk assessments as necessary to adequately mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation. Related controls: AC-2, AC-3, CM-7.

Control Enhancements:

1. The organization explicitly authorizes access to [Assignment: organization-defined list of security functions (deployed in hardware, software, and firmware) and security-relevant information].

Enhancement Supplemental Guidance: Establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters are examples of security functions. Explicitly authorized personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users. Related control: AC-17.

2. The organization requires that users of information system accounts, or roles, with access to all security functions, use non-privileged accounts, or roles, when accessing other system functions, and if feasible, audits any use of privileged accounts, or roles, for such functions.

Enhancement Supplemental Guidance: This control enhancement is intended to limit exposure due to operating from within a privileged account or role. The inclusion of *role* is intended to address those situations where an access control policy such as *Role Based Access Control (RBAC)* is being implemented and where a change of role provides the same degree of assurance in the change of access authorizations for both the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account. Audit of privileged activity may require physical separation employing information systems on which the user does not have privileged access.

References: None.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD AC-6 (1) (2)	HIGH AC-6 (1) (2)
-----------	-------------------------	-------------------------	--------------------------

AC-7 UNSUCCESSFUL LOGIN ATTEMPTS

Applicability: All Information Systems

Control: The information system:

- a. Enforces a limit of no more than three consecutive invalid login attempts, unless specified and allowed to be greater by DOI or NIST National Vulnerability Database (NVD) security configuration checklists and profiles (e.g., the USGCB and FDCC allow for no more than five consecutive invalid login attempts, and the enhancement supplemental guidance for the DOI Identification and Authentication IA-5 Authenticator Management control standard allows for mobile devices to be configured for ten failed login attempts under specified conditions after which they must be automatically wiped), by a user during a 15 minute period; and
- b. Automatically locks the account/node for 30 minutes when the maximum number of unsuccessful attempts is exceeded, unless specified and allowed to be less by DOI or NIST National Vulnerability Database (NVD) security configuration checklists and profiles (e.g., the USGCB and FDCC allow for automatic unlock after 15 minutes). The control applies regardless of whether the login occurs via a local or network connection.

Supplemental Guidance: Due to the potential for denial of service, automatic lockouts initiated by the information system are usually temporary and automatically release after a predetermined time period

established by the organization. If a delay algorithm is selected, the organization may chose to employ different algorithms for different information system components based on the capabilities of those components. Response to unsuccessful login attempts may be implemented at both the operating system and the application levels. This control applies to all accesses other than those accesses explicitly identified and documented by the organization in AC-14.

Control Enhancements: None.

References: NIST Federal Desktop Core Configuration (FDCC), United States Government Configuration Baseline (USGCB); Federal Risk and Authorization Management Program (FedRAMP) Cloud Computing Security Requirements Baseline.

Priority and Baseline Allocation:

P1	LOW AC-7	MOD AC-7	HIGH AC-7
-----------	-----------------	-----------------	------------------

AC-8 SYSTEM USE NOTIFICATION

Applicability: All Information Systems

Control: The information system:

- a. Displays an 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: (i) users are accessing a U.S. Government information system; (ii) system usage may be monitored, recorded, and subject to audit; (iii) unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) use of the system indicates consent to monitoring and recording;
- b. Retains the notification message or banner on the screen until users take explicit actions to log on to or further access the information system; and
- c. For publicly accessible systems: (i) displays the system use information when appropriate, before granting further access; (ii) displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and (iii) includes in the notice given to public users of the information system, a description of the authorized uses of the system.

Supplemental Guidance: System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the information system. System use notification is intended only for information system access that includes an interactive login interface with a human user and is not intended to require notification when an interactive interface does not exist. The DOI approved content for system use notification messages or banners is provided below.

WARNING TO USERS OF THIS SYSTEM

THIS IS A NOTICE OF MONITORING OF THE DEPARTMENT OF THE INTERIOR (DOI) INFORMATION SYSTEMS. This computer system, including all related equipment, networks, and network devices (including Internet access), is provided by the Department of the Interior (DOI) in accordance with the agency policy for official use and limited personal use.

All agency computer systems may be monitored for all lawful purposes, including but not limited to, ensuring that use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security. Any information on this computer system may be examined, recorded, copied and used for authorized purposes at any time.

All information, including personal information, placed or sent over this system may be monitored, and users of this system are reminded that such monitoring does occur. Therefore, there should be no expectation of privacy with respect to use of this system.

By logging into this agency computer system, you acknowledge and consent to the monitoring of this system. Evidence of your use, authorized or unauthorized, collected during monitoring may be used for civil, criminal, administrative, or other adverse action. Unauthorized or illegal use may subject you to prosecution.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	LOW AC-8	MOD AC-8	HIGH AC-8
-----------	-----------------	-----------------	------------------

AC-10 CONCURRENT SESSION CONTROL

Applicability: Moderate and High Impact Information Systems

Control: The information system limits the number of concurrent sessions for each system account to 1 session.

Supplemental Guidance: The organization may define the maximum number of concurrent sessions for an information system account globally, by account type, by account, or a combination. This control addresses concurrent sessions for a given information system account and does not address concurrent sessions by a single user via multiple system accounts.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P2	LOW Not Selected	MOD AC-10	HIGH AC-10
-----------	-------------------------	------------------	-------------------

AC-11 SESSION LOCK

Applicability: Moderate and High Impact Information Systems

Control: The information system:

- a. Prevents further access to the system by initiating a session lock after 15 minutes of inactivity or upon receiving a request from a user; and
- b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

Supplemental Guidance: A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence. The session lock is implemented at the point where session activity can be determined. This is typically at the operating system-level, but may be at the application-level. A session lock is not a substitute for logging out of the information system, for example, if the organization requires users to log out at the end of the workday.

Control Enhancements:

1. The information system session lock mechanism, when activated on a device with a display screen, places a publicly viewable pattern onto the associated display, hiding what was previously visible on the screen.

References: NIST Federal Desktop Core Configuration (FDCC), United States Government Configuration Baseline (USGCB); Federal Risk and Authorization Management Program (FedRAMP) Cloud Computing Security Requirements Baseline.

Priority and Baseline Allocation:

P3	LOW Not Selected	MOD AC-11 (1)	HIGH AC-11 (1)
-----------	-------------------------	----------------------	-----------------------

AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION/AUTHENTICATION

Applicability: All Information Systems

Control: The organization:

- a. Identifies specific user actions that can be performed on the information system without identification or authentication; and
- b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification and authentication.

Supplemental Guidance: This control is intended for those specific instances where an organization determines that no identification and authentication is required; it is not, however, mandating that such

instances exist in given information system. The organization may allow a limited number of user actions without identification and authentication (e.g., when individuals access public websites or other publicly accessible federal information systems such as <http://www.usa.gov>). Organizations also identify any actions that normally require identification or authentication but may under certain circumstances (e.g., emergencies), allow identification or authentication mechanisms to be bypassed. Such bypass may be, for example, via a software-readable physical switch that commands bypass of the login functionality and is protected from accidental or unmonitored use. This control does not apply to situations where identification and authentication have already occurred and are not being repeated, but rather to situations where identification and/or authentication have not yet occurred. Related control: CP-2, IA-2.

Control Enhancements:

1. The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission/business objectives.

References: None.

Priority and Baseline Allocation:

P1	LOW AC-14	MOD AC-14 (1)	HIGH AC-14 (1)
-----------	------------------	----------------------	-----------------------

AC-16 SECURITY ATTRIBUTES

Applicability: Moderate and High Impact Information Systems

Control: The information system supports and maintains the binding of **[Assignment: organization defined security attributes]** to information in storage, in process, and in transmission.

Control Enhancements: None mandated.

Priority and Baseline Allocation:

P0	LOW Not Selected	MOD AC-16	HIGH AC-16
-----------	-------------------------	------------------	-------------------

AC-17 REMOTE ACCESS

Applicability: All Information Systems

Control: The organization:

- a. Documents allowed methods of remote access to the information system;
- b. Establishes usage restrictions and implementation guidance for each allowed remote access method;
- c. Monitors for unauthorized remote access to the information system;
- d. Authorizes remote access to the information system prior to connection; and
- e. Enforces requirements for remote connections to the information system.

Supplemental Guidance: This control requires explicit authorization prior to allowing remote access to an information system without specifying a specific format for that authorization. For example, while the

organization may deem it appropriate to use a system interconnection agreement to authorize a given remote access, such agreements are not required by this control. Remote access is any access to an organizational information system by a user (or process acting on behalf of a user) communicating through an external network (e.g., the Internet). Examples of remote access methods include dial-up, broadband, and wireless (see AC-18 for wireless access). A virtual private network when adequately provisioned with appropriate security controls, is considered an internal network (i.e., the organization establishes a network connection between organization controlled endpoints in a manner that does not require the organization to depend on external networks to protect the confidentiality or integrity of information transmitted across the network). Remote access controls are applicable to information systems other than public web servers or systems specifically designed for public access. Enforcing access restrictions associated with remote connections is accomplished by control AC-3. Related controls: AC-3, AC-18, AC-20, IA-2, IA-3, IA-8, MA-4.

Control Enhancements:

1. The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods.

Enhancement Supplemental Guidance: Automated monitoring of remote access sessions allows organizations to audit user activities on a variety of information system components (e.g., servers, workstations, notebook/laptop computers) and to ensure compliance with remote access policy.

2. The organization uses cryptography to protect the confidentiality and integrity of remote access sessions.

Enhancement Supplemental Guidance: The encryption strength of mechanism is selected based on the security categorization of the information. Related controls: SC-8, SC-9, SC-13.

3. The information system routes all remote accesses through a limited number of managed access control points.

Enhancement Supplemental Guidance: Related control: SC-7.

4. The organization authorizes the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs and documents the rationale for such access in the security plan for the information system.

Enhancement Supplemental Guidance: Related control: AC-6.

5. The organization monitors for unauthorized remote connections to the information system continuously in real time, and takes appropriate action if an unauthorized connection is discovered.

7. The organization ensures that remote sessions for accessing *[Assignment: organization-defined list of security functions and security-relevant information]* employ *[Assignment: organization defined additional security measures]* and are audited.

Enhancement Supplemental Guidance: Additional security measures are typically above and beyond standard bulk or session layer encryption (e.g., Secure Shell [SSH], Virtual Private Networking [VPN] with blocking mode enabled). Related controls: SC-8, SC-9.

8. The organization disables tftp, (trivial ftp); X-Windows, Sun Open Windows; FTP; TELNET; IPX/SPX; NETBIOS; Bluetooth; RPC-services, like NIS or NFS; rlogin, rsh, rexec; SMTP (Simple Mail Transfer Protocol); RIP (Routing Information Protocol); DNS (Domain Name Services); UUCP (Unix- Unix Copy Protocol); NNTP (Network News Transfer Protocol); NTP (Network Time Protocol); Peer-to-Peer except for explicitly identified components in support of specific operational requirements.

Enhancement Supplemental Guidance: The organization can either make a determination of the relative security of the networking protocol or base the security decision on the assessment of other entities. Bluetooth and peer-to-peer networking are examples of less than secure networking protocols.

References: NIST Special Publications 800-46, 800-77, 800-113, 800-114, 800-121.

Priority and Baseline Allocation:

P1	LOW AC-17	MOD AC-17 (1) (2) (3) (4) (5) (7) (8)	HIGH AC-17 (1) (2) (3) (4) (5) (7) (8)
-----------	------------------	--	---

AC-18 WIRELESS ACCESS

Applicability: All Information Systems

Control: The organization:

- a. Establishes usage restrictions and implementation guidance for wireless access;
- b. Monitors for unauthorized wireless access to the information system;
- c. Authorizes wireless access to the information system prior to connection; and
- d. Enforces requirements for wireless connections to the information system.

Supplemental Guidance: Wireless technologies include, but are not limited to, microwave, satellite, packet radio (UHF/VHF), 802.11x, and Bluetooth. Wireless networks use authentication protocols (e.g., EAP/TLS, PEAP), which provide credential protection and mutual authentication. In certain situations, wireless signals may radiate beyond the confines and control of organization controlled facilities. Related controls: AC-3, IA-2, IA-3, IA-8.

Control Enhancements:

1. The information system protects wireless access to the system using authentication and encryption.

Enhancement Supplemental Guidance: Authentication applies to user, device, or both as necessary. Related control: SC-13.

2. The organization monitors for unauthorized wireless connections to the information system, including scanning for unauthorized wireless access points quarterly, and takes appropriate action if an unauthorized connection is discovered.

Enhancement Supplemental Guidance: Organizations proactively search for unauthorized wireless connections including the conduct of thorough scans for unauthorized wireless access points. The scan is not necessarily limited to only those areas within the facility containing the information

systems, yet is conducted outside of those areas only as needed to verify that unauthorized wireless access points are not connected to the system.

3. The organization disables, when not intended for use, wireless networking capabilities internally embedded within information system components prior to issuance and deployment.
4. The organization does not allow users to independently configure wireless networking capabilities.
5. The organization confines wireless communications to organization-controlled boundaries.

Enhancement Supplemental Guidance: Actions that may be taken by the organization to confine wireless communications to organization-controlled boundaries include: (i) reducing the power of the wireless transmission such that it cannot transit the physical perimeter of the organization; (ii) employing measures such as TEMPEST to control wireless emanations; and (iii) configuring the wireless access such that it is point to point in nature.

References: NIST Special Publications 800-48, 800-94, 800-97.

Priority and Baseline Allocation:

P1	LOW AC-18	MOD AC-18 (1) (2) (3)	HIGH AC-18 (1) (2) (3) (4) (5)
-----------	------------------	------------------------------	---------------------------------------

AC-19 ACCESS CONTROL FOR MOBILE DEVICES

Applicability: All Information Systems

Control: The organization:

- a. Establishes usage restrictions and implementation guidance for organization-controlled mobile devices;
- b. Authorizes connection of mobile devices meeting organizational usage restrictions and implementation guidance to organizational information systems;
- c. Monitors for unauthorized connections of mobile devices to organizational information systems;
- d. Enforces requirements for the connection of mobile devices to organizational information systems;
- e. Disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction;
- f. Issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures; and
- g. Applies [*Assignment: organization-defined inspection and preventative measures*] to mobile devices returning from locations that the organization deems to be of significant risk in accordance with organizational policies and procedures.

Supplemental Guidance: Mobile devices include portable storage media (e.g., USB memory sticks, external hard disk drives) and portable computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices). Organization-controlled mobile devices include those devices for which the organization has the authority to specify and the ability to enforce specific security requirements. Usage restrictions and implementation guidance related to mobile devices include, for

example, configuration management, device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared). Examples of information system functionality that provide the capability for automatic execution of code are AutoRun and AutoPlay.

Organizational policies and procedures for mobile devices used by individuals departing on and returning from travel include, for example, determining which locations are of concern, defining required configurations for the devices, ensuring that the devices are configured as intended before travel is initiated, and applying specific measures to the device after travel is completed. Specially configured mobile devices include, for example, computers with sanitized hard drives, limited applications, and additional hardening (e.g., more stringent configuration settings). Specified measures applied to mobile devices upon return from travel include, for example, examining the device for signs of physical tampering and purging/reimaging the hard disk drive. Protecting information residing on mobile devices is covered in the media protection family. Related controls: MP-4, MP-5.

Control Enhancements:

1. The organization restricts the use of writable, removable media in organizational information systems.
2. The organization prohibits the use of personally owned, removable media in organizational information systems.
3. The organization prohibits the use of removable media in organizational information systems when the media has no identifiable owner.

Enhancement Supplemental Guidance: An identifiable owner (e.g., individual, organization, or project) for removable media helps to reduce the risk of using such technology by assigning responsibility and accountability for addressing known vulnerabilities in the media (e.g., malicious code insertion).

References: NIST Special Publications 800-114, 800-124.

Priority and Baseline Allocation:

P1	LOW AC-19	MOD AC-19 (1) (2) (3)	HIGH AC-19 (1) (2) (3)
-----------	------------------	------------------------------	-------------------------------

AC-20 USE OF EXTERNAL INFORMATION SYSTEMS

Applicability: All Information Systems

Control: The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:

- a. Access the information system from the external information systems; and
- b. Process, store, and/or transmit organization-controlled information using the external information systems.

Supplemental Guidance: External information systems are information systems or components of information systems that are outside of the authorization boundary established by the organization and for which the organization typically has no direct supervision and authority over the application of required security controls or the assessment of security control effectiveness. External information systems include, but are not limited to: (i) personally owned information systems (e.g., computers, cellular telephones, Smartphones, personal digital assistants or personal electronic devices (PDAs/PEDs), etc.); (ii) privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, convention centers, or airports); (iii) information systems owned or controlled by nonfederal governmental organizations; and (iv) federal information systems that are not owned by, operated by, or under the direct supervision and authority of the organization. For some external systems, in particular those systems operated by other federal agencies, including organizations subordinate to those agencies, the trust relationships that have been established between those organizations and the originating organization may be such, that no explicit terms and conditions are required. In effect, the information systems of these organizations would not be considered external. These situations typically occur when, for example, there is some pre-existing sharing or trust agreement (either implicit or explicit) established between federal agencies and/or organizations subordinate to those agencies, or such trust agreements are specified by applicable laws, Executive Orders, directives, or policies. Authorized individuals include organizational personnel, contractors, or any other individuals with authorized access to the organizational information system and over which the organization has the authority to impose rules of behavior with regard to system access. The restrictions that an organization imposes on authorized individuals need not be uniform, as those restrictions are likely to vary depending upon the trust relationships between organizations. Thus, an organization might impose more stringent security restrictions on a contractor than on a state, local, or tribal government.

This control does not apply to the use of external information systems to access public interfaces to organizational information systems and information (e.g., individuals accessing federal information through www.usa.gov). The organization establishes terms and conditions for the use of external information systems in accordance with organizational security policies and procedures. The terms and conditions address as a minimum; (i) the types of applications that can be accessed on the organizational information system from the external information system; and (ii) the maximum security categorization of information that can be processed, stored, and transmitted on the external information system. This control defines access authorizations enforced by AC-3, rules of behavior requirements enforced by PL-4, and session establishment rules enforced by AC-17. Related controls: AC-3, AC-17, PL-4.

Control Enhancements:

1. The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization:
 - a. Can verify the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or
 - b. Has approved information system connection or processing agreements with the organizational entity hosting the external information system.
2. The organization limits the use of organization-controlled portable storage media by authorized individuals on external information systems.

Enhancement Supplemental Guidance: Limits on the use of organization-controlled portable storage media in external information systems can include, for example, complete prohibition of the use of such devices or restrictions on how the devices may be used and under what conditions the devices may be used.

All sensitive agency information, including Personally Identifiable Information (PII), shall only be processed, housed, transmitted or stored using DOI controlled and managed computing and network resources. To clarify, this does not imply that agency employees or contractors are required to use Government Furnished Equipment (GFE) computers or devices as there are many options available within which this requirement can be met. The intent of the requirement is that it is the sensitive information that requires adequate protection and to be able to ensure its protection the agency can only do so by ensuring that it effectively manages the resources that afford such information/data adequate protection. Examples of some options to meet the requirement might include:

- The agency deploying and managing virtualized secured client operating systems on personally owned (non-GFE) computers where the configuration management and control over such virtual environments is managed by the agency while the employee retains control over their own non-virtualized operating system configuration. The virtualized environment should be configured to prevent any sensitive agency information from being saved to, or stored on, the personally owned computer outside of the protected virtual environment and its encrypted data/information storage allocated for use and accessible only by the virtual environment.
- The agency providing technology that includes secure virtualized operating system environments and encrypted storage that resides solely on a security hardened USB Thumb-drive.
- The agency providing approved technology that securely enables remote access of internal agency computer or network resources on which to perform assigned work (e.g., Citrix) that virtualizes user session and prevents downloading, copying, printing, screen capturing, etc. of any data/information locally at the remote location.

Requiring use of only agency GFE computers is an option where the above, or similar secure operating capabilities, are not available or otherwise viable.

Agency employees and contractors are permitted to use their own Internet Service Providers (ISPs) to connect to the agency’s approved enterprise remote access solutions that provide encrypted communication tunnels for the secure transport (transmission) of any sensitive agency information between the connecting system and the agency network computing environment. Similarly, agency employees and contractors are permitted to use their home, or other, Wi-Fi connections to establish Internet connectivity and connect to the agency’s enterprise remote access solutions provided those connections employ authenticated, encrypted, and secure configurations that are compliant with applicable standards (i.e., the most current versions of NIST FIPS 140, *Security Requirements for Cryptographic Modules*; Best Practice Security Recommendations specified in NIST SP 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*; NIST SP 800-114, *User’s Guide to Securing External Devices for Telework and Remote Access*; and NIST SP 800-46, *Guide to Enterprise Telework and Remote Access Security*) to minimize the likelihood that the computing resources they are using are not susceptible to direct attack.

References: FIPS Publication 199.

Priority and Baseline Allocation:

P1	LOW AC-20	MOD AC-20 (1) (2)	HIGH AC-20 (1) (2)
-----------	------------------	--------------------------	---------------------------

AC-22 PUBLICLY ACCESSIBLE CONTENT

Applicability: All Information Systems

Control: The organization:

- a. Designates individuals authorized to post information onto an organizational information system that is publicly accessible;
- b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;
- c. Reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the organizational information system;
- d. Reviews the content on the publicly accessible organizational information system for nonpublic information quarterly; and
- e. Removes nonpublic information from the publicly accessible organizational information system, if discovered.

Supplemental Guidance: Nonpublic information is any information for which the general public is not authorized access in accordance with federal laws, Executive Orders, directives, policies, regulations, standards, or guidance. Information protected under the Privacy Act and vendor proprietary information are examples of nonpublic information. This control addresses posting information on an organizational information system that is accessible to the general public, typically without identification or authentication. The posting of information on non-organization information systems is covered by appropriate organizational policy. Related controls: AC-3, AU-13.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P2	LOW AC-22	MOD AC-22	HIGH AC-22
-----------	------------------	------------------	-------------------