Docusign Envelope ID: 1636BF85-DA76-4F0E-964C-4C3DA19ABB87

IT Security Procedural Guide: Access Control (AC) CIO-IT Security-01-07

Revision 7

February 10, 2025

Office of the Chief Information Security Officer

Docusign Envelope ID: 1636BF85-DA76-4F0E-964C-4C3DA19ABB87

VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
		Revision 2 – January 30, 2008		
1	Scott/Heard	Changes made throughout the document to reflect FISMA, NIST and GSA CIO P 2100.1B requirements.	Updated to reflect and implement various FISMA, NIST and GSA CIO P 2100.1B requirements.	Various
2	Scott/Heard	Changes throughout the document to correspond with revisions made to CIO-IT Security-01-09, CIO-IT Security-06-30 and CIO-IT Security-01-04.	Updated to reflect the correlation of the CIO-IT Security Guides; and to further express policy within them as standalone documents	Various
3	Hummel/ Windelberg	Changes throughout the document to correspond with update of the current version of GSA CIO P 2100	The most current version of GSA CIO P 2100 and more detailed guidance on implementing policy	Various
		Revision 3 – April 1, 2015		
1	Sitcharing	Changes throughout to correspond with revisions made to CIO-IT-Security-06-30.	Updated to reflect correlation of the CIO-IT Security Guide and CIO P 2100.1.	Throughout
2	Heard	Changes the document to Implement ADM O 5440.667	Updated to reflect CISO GSA IT responsibilities	Throughout
3	Heard/Mott	Privacy access information included	Appendix J controls included in table 1 as well as explained within the guide	Throughout
		Revision 4 – May 8, 2017		
1	Feliksa/Dean/ Klemens	Update to current format, style, and policies.	Updated to latest guide structure. Revised to reflect updates to Federal policies, NIST documents, and GSA processes.	Throughout
		Revision 5 – August 18, 2022		
1	Dean/ McCormick/ Klemens	Revisions include: • Updated to NIST SP 800-53, Revision 5 controls, GSA parameters, and implementation statements. • Updated format, style, and content.	Align to current NIST and GSA guidance and GSA parameters. New or substantively changed controls in Revision 5 are: AC-2, AC-2(1), AC-2(4), AC-2(5, AC-2(13), AC-3(14), AC-4(4), AC-6(1), AC-6(7), AC-7, AC-11, AC-17(4), AC-18(3), AC-20, AC-20(2).	Throughout
		Revision 6 - May 14, 2024		
1	McCormick/ Klemens	Revisions include: • Updated AC-08, System Use Notification, to align with OMB M-23-22. • Added OMB M-23-22 to references.	Align to current Federal and GSA guidance.	15-17
2	Klemens	• Various editorial updates.		Throughout
		Revision 7 - February 10, 2025		
1	Normand/ Klemens/ Peralta	• Added mini tables to control sections to ease the determination of control applicability. • Updated guidance for controls: AC-18, AC-19, AC-20, AC-20(01), and AC-20(02), to align with the Common Control Catalog (CCC), and removed AC-02(06) to align with GSA's CTW.	Align to current Federal and GSA guidance.	Throughout

Docusign Envelope ID: 1636BF85-DA76-4F0E-964C-4C3DA19ABB87

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
		• Moved policy, references, and roles and responsibilities to appendices.		

Docusign Envelope ID: 1636BF85-DA76-4F0E-964C-4C3DA19ABB87

Approval

IT Security Procedural Guide: Access Control (AC), CIO-IT Security-01-07, Revision 7, is hereby approved for distribution.

DocuSigned by:
parimala rao
122A567B868C4F0...

Parimala Rao
Acting GSA Chief Information Security Officer

Contact: GSA Office of the Chief Information Security Officer (OCISO), Policy and Compliance Division (ISP) at ispcompliance@gsa.gov.

Docusign Envelope ID: 1636BF85-DA76-4F0E-964C-4C3DA19ABB87

Table of Contents

Note: Hyperlinks in running text will be provided if they link to a location within this document (i.e., a different section). Hyperlinks will be provided for external sources unless the hyperlink is to a web page or document listed in Appendix C. For example, Google Forms, Google Docs, and websites will have links.

Docusign Envelope ID: 1636BF85-DA76-4F0E-964C-4C3DA19ABB87

1 Introduction

Implementing an effective access control program adhering to General Services Administration (GSA) Order CIO 2100.1, “GSA Information Technology (IT) Security Policy” and federal mandates is the best way to ensure the protection of GSA systems and resources from loss, misuse, disclosure, or impairment. An effective program carefully applies necessary controls to ensure that users are given access only to data and resources as needed and allowed by policy and authorization. Effective access control is implemented by a combination of personnel, physical, and logical practices, procedures, features, and mechanisms. This guide focuses on logical access controls as defined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, “Security and Privacy Controls for Information Systems and Organizations”, in the Access Control (AC) family of security controls. Physical access controls are covered in CIO-IT Security-12-64: Physical and Environmental Protection. Personnel access controls are covered in CIO-IT Security-18-90: Common Control Catalog (CCC) and GSA’s personnel security policies.

Every GSA system across all Service and Staff Offices (SSOs) must follow the practices described in this guide. Any deviations from the security requirements established in CIO 2100.1 must be coordinated by the appropriate Information Systems Security Officer (ISSO) through the appropriate Information Systems Security Manager (ISSM) and approved by the Authorizing Official (AO). Any deviations, exceptions, or other conditions not following GSA policies and standards must be submitted using the Security Deviation Request Google Form.

The access control principles and practices described in this guide are based on guidance from NIST, including NIST SP 800-53, Revision 5. This guide provides an overview of access control, roles and responsibilities, NIST SP 800-53, Revision 5 access control requirements per Federal Information Processing Standards (FIPS) Publication 199, “Standards for Security Categorization of Federal Information and Information Systems”, security categorization level, and procedures for implementing these requirements.

Executive Order (EO) 13800, Presidential Executive Order on “Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,” requires all agencies to use “The Framework for Improving Critical Infrastructure Cybersecurity (the Framework) developed by NIST or any successor document to manage the agency’s cybersecurity risk.” This NIST document is commonly referred to as the Cybersecurity Framework (CSF). The GSA uses the NIST SP 800-37, Revision 2, “Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,” commonly referred to as the Risk Management Framework (RMF) as its foundation for managing risk, assessment and authorization (A&A) of systems, and the implementation of NIST SP 800-53, Revision 5 controls. Further information on how AC controls relate to the CSF is provided in Appendix A.

Note: The GSA is in the process of developing and updating CIO 2100.1 to align to CSF 2.0, once that process is completed, the next version of this guide will align to CSF 2.0.

1.1 Purpose

The purpose of this guide is to provide guidance for the AC controls identified in NIST SP 800-53 and access control requirements specified in CIO 2100.1. The guide provides GSA Federal employees, contractors with significant security responsibilities (as identified in CIO 2100.1), and other IT personnel involved in implementing access control, guidance on the specific

Docusign Envelope ID: 1636BF85-DA76-4F0E-964C-4C3DA19ABB87

procedures they are to follow for implementing AC features and functions for systems under their purview.

1.2 Scope

The requirements outlined within this guide apply to and must be followed by all GSA Federal employees and contractors who are involved in implementing access control features and functions for GSA systems and information. All GSA systems must adhere to the requirements and guidance provided with regard to the procedures, processes, and methods for implementing access control as described in this guide. Per CIO 2100.1, a system is a system used or operated:

- by the GSA; or
- on behalf of the GSA by a contractor of GSA or by another organization.

1.3 Policy

Appendix B contains the CIO 2100.1 policy statements regarding access control, privilege management, and user account management.

1.4 References

Appendix C provides links to references used throughout this guide.

1.5 Access Control Roles and Responsibilities

Appendix D provides a listing of the roles and responsibilities related to implementing, administering, and managing access control at the GSA.

2 Access Control Overview

2.1 What Are Access Controls

Access control, as it relates to this guide, pertains to granting or denying logical access to a resource, such as data/information or a system. Access is typically gained by an individual (a user of the resource), for example a GSA employee or a contractor; sometimes individuals are aggregated into groups. It is also possible to have automated system-to-system access, known as a system interconnection.

Identification, authentication, and authorization are key terms regarding access control. Each user of a resource should have a unique identifier (e.g., user ID). In some situations, access for anonymous users may be considered as an option. However, this type of access must be based on a sound risk management decision, with documented controls and approved by the AO of the resource. Authentication involves verifying a user (or device) identity through mechanisms such as Personal Identity Verification (PIV) cards, passwords, etc. More details about identification and authentication are available in CIO-IT Security-01-01: Identification and Authentication (I&A) determines what the individual or device is allowed and is not allowed to do with the resource, such as view the resource but not delete it.

An access control list (ACL) specifies what access rights are permitted to a user. Groups of users may also be classified by assigned and documented roles and the access rights may be

Docusign Envelope ID: 1636BF85-DA76-4F0E-964C-4C3DA19ABB87

assigned to the roles; in role-based access controls, users obtain only the rights assigned to the group (role) as a whole.

2.2 Why Access Controls Are Important

Employing effective access controls based on sound risk management decisions protects GSA resources from internal and external threats and provides a level of assurance that the agency can successfully perform its mission.

Effective access controls also improve the overall security posture of the GSA by:

- Ensuring the confidentiality, integrity, and availability of IT resources and data;
- Enhancing the ability to determine where a breach has occurred;
- Creating greater individual accountability for personnel;
- Limiting user access only to needed information required to perform specific responsibilities (i.e., need-to-know/need-to-share, least privilege access);
- Limiting access to sensitive resources (e.g., financial records, personally identifiable information (PII), security software programs, or data centers).
- Ensuring the GSA complies with Federal regulations and mandates.

Without effective access controls, the GSA increases the possibility of information loss or theft, regardless of its sensitivity, and limits its ability to control who has access to information.

Confidentiality, integrity, and availability of information are also an issue when access controls are not properly implemented. If a security breach affects one area of the network, and there are insufficient access controls present to contain or mitigate the breach, its reach may be expanded, affecting additional systems, components, and data. Improperly implemented access controls can result in negative consequences, ranging from a lack of information being available to compromised data integrity and/or lack of confidentiality. There is also a possibility of a negative financial impact due to the response to or recovery from a breach. Furthermore, legal issues may also occur for not complying with laws and regulations, resulting in regulatory admonishment, fines and more.

Ineffective access controls also hinder accountability for the actions of users of an IT resource, whether it is a system or its information. Appendix E provides information on access control best practices.

3 Implementation Guidance for AC Controls

In the implementation guidance text, the GSA-defined parameter settings included in the control requirements are in blue text and offset by brackets. As stated in Section 1.2, Scope, the requirements outlined within this guide apply to all GSA systems and must be followed by all GSA Federal employees and contractors involved in managing access control for GSA information systems and data. The GSA implementation guidance stated for each control applies to personnel and/or the information systems operated on behalf of the GSA. Any additional instructions or requirements for vendor/contractor systems will be included in a Vendor/Contractor System-Specific Expectations portion of the appropriate control section.

Table 3-1 identifies the designation of AC controls as Common, Hybrid, or System-Specific controls for Federal and Contractor systems. Effectively, common controls are provided by the GSA at the enterprise level or by one of GSA's Major Information Systems (e.g., General

Docusign Envelope ID: 1636BF85-DA76-4F0E-964C-4C3DA19ABB87

Support System), system-specific controls are implemented at the system level, and hybrid controls have shared responsibilities. CIO-IT Security 18-90, the CCC, describes the GSA enterprise-wide controls and outlines the responsible parties for implementing them.

Table 3-1. Designation of AC Controls

System Type	Federal	Contractor
Common	AC-01, AC-02(05), AC-19(05), AC-20(02)	AC-02(05), AC-19(05), AC-20(02)
Hybrid	AC-19	AC-01, AC-19
System-Specific	AC-02, AC-02(01), AC-02(02), AC-02(03), AC-02(04), AC-02(07), AC-02(11), AC-02(12), AC-02(13), AC-03, AC-03(14), AC-04, AC-05, AC-06, AC-06(01), AC-06(02), AC-06(03), AC-06(05), AC-06(07), AC-06(09), AC-06(10), AC-07, AC-08, AC-10, AC-11, AC-11(01), AC-12, AC-14, AC-17, AC-17(01), AC-17(02), AC-17(03), AC-17(04), AC-18, AC-18(01), AC-18(03), AC-18(04), AC-18(05), AC-20, AC-20(01), AC-22	AC-02, AC-02(01), AC-02(02), AC-02(03), AC-02(04), AC-02(07), AC-02(11), AC-02(12), AC-02(13), AC-03, AC-03(14), AC-04, AC-05, AC-06, AC-06(01), AC-06(02), AC-06(03), AC-06(05), AC-06(07), AC-06(09), AC-06(10), AC-07, AC-08, AC-10, AC-11, AC-11(01), AC-12, AC-14, AC-17, AC-17(01), AC-17(02), AC-17(03), AC-17(04), AC-18, AC-18(01), AC-18(03), AC-18(04), AC-18(05), AC-20, AC-20(01), AC-21, AC-22

Table 3-2 identifies GSA's AC control applicability at the FIPS 199 Low, Moderate, and High levels, and for GSA's Lightweight (LATO) and Moderate Impact Software-as-a Service (MiSaaS) authorization processes.

Table 3-2: AC Control Applicability

FIPS 199 Level/A&A Process	Applicable Controls
Low	AC-01, AC-02, AC-03, AC-07, AC-08, AC-14, AC-17, AC-18, AC-19, AC-20, AC-22
Moderate	AC-01, AC-02, AC-02(01), AC-02(02), AC-02(03), AC-02(04), AC-02(05), AC-02(13), AC-03, AC-03(14)^, AC-04, AC-05, AC-06, AC-06(01), AC-06(02), AC-06(05), AC-06(07), AC-06(09), AC-06(10), AC-07, AC-08, AC-11, AC-11(01), AC-12, AC-14, AC-17, AC-17(01), AC-17(02), AC-17(03), AC-17(04), AC-18, AC-18(01), AC-18(03), AC-19, AC-19(05), AC-20, AC-20(01), AC-20(02), AC-21, AC-22
High	AC-01, AC-02, AC-02(01), AC-02(02), AC-02(03), AC-02(04), AC-02(05), AC-02(11), AC-02(12), AC-02(13), AC-03, AC-03(14)^, AC-04, AC-04(04), AC-05, AC-06, AC-06(01), AC-06(02), AC-06(03), AC-06(05), AC-06(07), AC-06(09), AC-06(10), AC-07, AC-08, AC-10, AC-11, AC-11(01), AC-12, AC-14, AC-17, AC-17(01), AC-17(02), AC-17(03), AC-17(04), AC-18, AC-18(01), AC-18(03), AC-18(04), AC-18(05), AC-19, AC-19(05), AC-20, AC-20(01), AC-20(02), AC-21, AC-22
LATO	AC-02, AC-03, AC-03(14)^, AC-06(05), AC-06(09)
MiSaaS	AC-02, AC-02(07), AC-03, AC-03(14)^, AC-05, AC-06, AC-06(02), AC-06(09), AC-08, AC-12, AC-21

^-control is applicable if PII is stored, processed, or transmitted

Docusign Envelope ID: 1636BF85-DA76-4F0E-964C-4C3DA19ABB87

For readers' ease of use, "mini tables" (see Table 3-3) that contain control/enhancement designation and applicability information are provided at the end of control statements for each AC control. The tables allow readers to see if a control/enhancement is applicable at their system's FIPS Level/A&A process and if it is common (C), Hybrid (H), or system specific (S), eliminating the need to refer back to Tables 3-1 and 3-2 for this information.

Table 3-3: Example Mini Table

	Low	Mod	High	LATO	MiSaaS	Federal	Contractor
Control ID	✓	✓	✓			C	H

3.1 AC-01 Access Control Policy and Procedures

Control:

a. Develop, document, and disseminate to [personnel with IT security responsibilities as defined in GSA Order CIO 2100.1]:
   1. [Organization-level] access control policy that:
      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
   2. Procedures to facilitate the implementation of the access control policy and the associated contingency planning controls;

b. Designate an [CISO] to manage the development, documentation, and dissemination of the access control policy and procedures; and

c. Review and update the current access control:
   1. Policy [annually, as part of CIO 2100.1 update] and following [changes to Federal or GSA policies, requirements, or guidance]; and
   2. Procedures [at least every three (3) years] and following [changes to Federal or GSA policies, requirements, or guidance].

	Low	Mod	High	LATO	MiSaaS	Federal	Contractor
AC-01	✓	✓	✓			C	H

Common Control Implementation:
The GSA access control policy is defined in GSA Order CIO 2100.1, "GSA Information Technology (IT) Security Policy," which addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance regarding access control for GSA systems. This policy is disseminated GSA-wide via GSA's InSite centralized agency Directives Library website.

Access control procedures are documented in CIO-IT Security-01-07: Access Control. This guide is disseminated GSA-wide via GSA's InSite centralized agency IT Security Procedural Guides website.

Per CIO 2100.1, the CISO is responsible for managing the development and publishing of all security policies and IT security procedural guides.

Docusign Envelope ID: 1636BF85-DA76-4F0E-964C-4C3DA19ABB87

The GSA OCISO is responsible for reviewing and updating CIO 2100.1 annually and following changes to Federal or GSA policies, requirements, or guidance. CIO-IT Security-01-07 every three years and following changes to Federal or GSA policies, requirements, or guidance.

Federal System System-Specific Expectation:
None, common control.

Vendor/Contractor System-Specific Expectation:
Vendors/Contractors may defer to the GSA policy and guide or implement their own access control policies and procedures which comply with GSA's requirements with the approval of the Authorizing Official (AO).

3.2 AC-02 Account Management

Control:

a. Define and document the types of accounts allowed and specifically prohibited for use within the system;
b. Assign account managers;
c. Require [GSA SSO or Contractor recommended prerequisites and criteria (based on defined user role(s) matrix in GSA SSPP Template Section 9: Types of Users) as approved by the CISO and AO] for group and role membership;
d. Specify:
    1. Authorized users of the system;
    2. Group and role membership; and
    3. Access authorizations (i.e., privileges) and [the following attributes as defined in the user role(s) matrix in GSA SSPP Template Section 9: Types of Users - Internal or External; Privileged (P), Non-Privileged (NP), or No Logical Access (NLA); Sensitivity Level; Authorized Privileges; Functions Performed; MFA Authentication Method] for each account;
e. Require approvals by [designated account managers as specified in AC-02.b] for requests to create accounts;
f. Create enable, modify, disable, and remove accounts in accordance with [CIO-IT Security-01-01, Identification and Authentication, CIO-IT Security-01-07, Access Control, and GSA-defined procedures or conditions (as applicable)];
g. Monitor the use of accounts;
h. Notify account managers and [System Owner, System/Network Administrator, and/or ISSO] within:
    1. [14 days] when accounts are no longer required;
    2. [14 days] when users are terminated or transferred; and
    3. [14 days] when system usage or need-to-know changes for an individual;
i. Authorize access to the system based on:
    1. A valid access authorization;
    2. Intended system usage; and
    3. [Role privileges identified in GSA SSPP Section 9: Types of Users];
j. Review accounts for compliance with account management requirements [annually];
k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and
l. Align account management processes with personnel termination and transfer processes.

Control Enhancements:

Docusign Envelope ID: 1636BF85-DA76-4F0E-964C-4C3DA19ABB87

(01) Account Management | Automated System Account Management. Support the management of system accounts using [GSA SSO or Contractor recommended automated mechanisms as approved by the GSA CISO and AO];
(02) Account Management | Automated Temporary and Emergency Account Management. Automatically [disable] temporary and emergency accounts after [no more than 90 days];
(03) Account Management | Disable Accounts. Disable accounts within [30 days for GSA users; for non-GSA users as determined by the System Owner and approved by GSA CISO and AO] when the accounts:
  (a) Have expired;
  (b) Are no longer associated with a user or individual;
  (c) Are in violation of organization policy; or
  (d) Have been inactive for [90 days for GSA users; for non-GSA users as determined by the System Owner and approved by the GSA CISO and AO].
(04) Account Management | Automated Audit Actions. Automatically audit account creation, modification, enabling, disabling, and removal actions;
(05) Account Management | Inactivity Logout. Require that users log out when [they have completed their workday];
(07) Account Management | Privileged User Accounts
  (a) Establish and administer privileged user accounts in accordance with [a role-based or attribute-based access schema];
  (b) Monitor privileged role or attribute assignments;
  (c) Monitor changes to roles or attributes;
  (d) Revoke access when privileged role or attribute assignments are no longer appropriate.
(11) Account Management | Usage Conditions. Enforce [GSA SSO or Contractor recommended circumstances and/or usage conditions to be approved by the GSA CISO and AO] for [GSA SSO or Contractor recommended system accounts to be approved by the GSA CISO and AO].
(12) Account Management | Account Monitoring for Atypical Usage.
  (a) Monitor system accounts for [atypical times of day and originating IP address for a known privileged account user that are inconsistent with normal usage patterns]; and
  (b) Report atypical usage of system accounts to [the ISSO and the GSA OCISO].
(13) Account Management | Disable Accounts for High-Risk Individuals. Disable accounts of individuals posing a significant risk within [24 hours] of discovery of [account compromise relating to an incident or Insider Threat event (per the OMA Insider Threat Program) as directed but the GSA CISO, AO, and/or GSA Incident Response Team].

	Low	Mod	High	LATO	MiSaaS	Federal	Contractor
AC-02	✓	✓	✓	✓	✓	S	S
AC-02(01)		✓	✓			S	S
AC-02(02)		✓	✓			S	S
AC-02(03)		✓	✓			S	S
AC-02(04)		✓	✓			S	S
AC-02(05)		✓	✓			C	C
AC-02(07)					✓	S	S
AC-02(11)			✓			S	S

Docusign Envelope ID: 1636BF85-DA76-4F0E-964C-4C3DA19ABB87

	Low	Mod	High	LATO	MiSaaS	Federal	Contractor
AC-02(12)			✓			S	S
AC-02(13)		✓	✓			S	S

Common Control Implementation:
AC-02(05) is a policy-based Common Control provided by GSA Order CIO 2104.1, "GSA Information Technology (IT) General Rules of Behavior" Category Access - (3) Logoff and shutdown your GSA workstation at the end of the workday.

Inactivity logout is behavior- or policy-based and requires users to take physical action to log out when they expect to be inactive longer than a defined period of time. A system's automatic enforcement of user inactivity logout is documented by AC-11.

System-Specific Expectations:
The focus of AC-02 is maintaining control over who is able to access GSA system resources to protect against internal and external threats. The first step in this process is to identify the types of users for the system, this is documented in Section 9.4 of GSA's SSPP templates. Account types documented therein are allowed, any account that is not documented is not allowed (prohibited), e.g., group, shared accounts. Account managers for systems are designated by the System Owner in collaboration with the data owner. Access must be requested for any individual and their need-to-know/need-to-share documented in order for an account to be provided. As specified in the control parameter for part c of the control any prerequisites and criteria for role membership and associated privileges must be documented and approved.

GSA's default access to any resource is DENY. ALLOW access is granted based on the approved role and privileges an account for a user is provisioned when an account is created. When account requests are approved, the ISSO and the appropriate administrators are responsible for establishing accounts with unique account identifiers; shared accounts are not allowed.

Establishing, maintaining, and removing access rights to GSA systems in accordance with GSA-defined procedures must be conducted by system/network administrators, in conjunction with system and Data Owners, ISSMs and ISSOs. All allowed accounts must be documented and defined and include group and role memberships and access authorizations. Account usage is monitored by tracking activity, details on monitoring activity (i.e., auditing/logging) can be found in CIO-IT Security-01-08: Audit and Accountability (AU).

Supervisors of users must notify account managers and System Owners, system/network administrators, and ISSOs within two weeks of when an account change is required. For example, if an individual transfers, terminates, or their relationship to GSA or to a GSA system changes under any circumstances, accounts and authorization rights must be reviewed and modifications, disablement, or revocation of their accounts made, as appropriate.

On an annual basis ISSOs must coordinate with System Owners and Data Owners to validate continued need for an individual's account to access a system as well as the roles and privileges for the individual/account. The ISSO must coordinate with administrators and account managers, as appropriate, when modifications are required based on the review. Similarly, when an individual leaves a group, any group account authenticators must be changed to ensure that former group members do not retain access. CIO-IT Security-03-23: Termination and Transfer contains information on handling personnel terminations and transfers.

Docusign Envelope ID: 1636BF85-DA76-4F0E-964C-4C3DA19ABB87

For AC-02(01), systems must manage accounts using automated mechanisms, the approval of which is based on the assessment conducted as part of the system's ATO process. For example, the use of automated mechanisms to identify inactive accounts is one use case.

For AC-02(02), systems must disable temporary and emergency accounts after no more than 90 days. For example, if possible, any emergency or temporary account should be set to automatically expire in 90 days, otherwise a manual process will have to be established.

For AC-02(03), GSA user accounts that are no longer associated with a user, are expired, are in violation of GSA policy, or have been inactive for 90 days must be disabled within 30 days. For non-GSA users the time period for disablement can be determined by the System Owner, but it must be approved by the GSA CISO and AO. If appropriate, restored access for disabled accounts may be requested by the user.

For AC-02(04), system account actions (creation, modification, enabling, disabling, removal) must be automatically audited. Additional information on auditing can be found in CIO-IT Security-01-08.

For AC-02(07), systems following the MiSaaS process must follow a role-based or attribute-based access scheme to establish and administer privileged user accounts. A process must be established to monitor role and attribute assignments and changes to them. Access must be revoked when privileged roles or attribute assignments are no longer needed. For example, when an individual's role changes, the role assignment and/or attributes must reflect and change between the previous and new role.

For AC-02(11), systems must enforce any circumstances or usage conditions for specified accounts that have been approved by the GSA CISO and AO. For example, if a specific account is only to be used at certain times of the month, the system should be configured to only allow its use during that time.

For AC-02(12), privileged accounts must be monitored for atypical usage (e.g., time of day, originating IP address) that differ from that account's normal patterns. Since such activity could be an indicator of an insider or external threat, this behavior must be reported to the ISSO and the GSA OCISO (i.e., Incident Response Team).

For AC-02(13), system accounts belonging to individuals who pose a significant risk must be disabled within 24 hours after it has been discovered that there has been an incident related to an account compromise or a credible insider threat has been identified per GSA's Insider Threat Program. Accounts should only be disabled as directed by the GSA CISO, AO, and/or Incident Response Team.

3.3 AC-03 Access Enforcement

Control: Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

Control Enhancements:

(14) Access Enforcement | Individual Access. Provide [a self service mechanism or use GSA's Privacy Act Request for Access process] to enable individuals to have access to

Docusign Envelope ID: 1636BF85-DA76-4F0E-964C-4C3DA19ABB87

the following elements of their personally identifiable information: [as defined in the GSA PII Rules Matrix].

	Low	Mod	High	LATO	MiSaaS	Federal	Contractor
AC-03	✓	✓	✓	✓	✓	S	S
AC-03(14)		✓^	✓^	✓^	✓^	S	S

^-control is applicable if PII is stored, processed, or transmitted

System-Specific Guidance:
For AC-03, GSA systems must be configured to enforce the access that users and processes have to system resources (e.g., devices, files, records). Systems are responsible for administering the user identification, authentication, and authorization scheme used in the system. Authenticators must follow GSA policies per GSA Orders CIO 2100.1, CIO 2183.1, "Enterprise Identity, Credential, and Access Management (ICAM) Policy," and CIO-IT Security-01-01.

For AC-03(14), systems with PII must provide users with the ability to access personally identifiable information about themselves to understand how their information is being used and to ensure it is accurate. As stated in the control parameter, GSA PII Rules Matrix identifies PII for the GSA and either a self service mechanism provided by the system or GSA's Privacy Act Request Access process can be used to satisfy the control requirement.

3.4 AC-04 Information Flow Enforcement

Control: Enforce approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Web Services Security (WS Security), WS-Security Policy, WS Trust, WS Policy Framework, Security Assertion Markup Language (SAML), and extensible Access Control Markup Language (XACML)].

Control Enhancements:

(04) Information Flow Enforcement | Flow Control of Encrypted Information. Prevent encrypted information from bypassing [any information flow control mechanisms] by [decrypting the information, blocking the flow of the encrypted information, or by terminating communications sessions attempting to pass encrypted information].

	Low	Mod	High	LATO	MiSaaS	Federal	Contractor
AC-04		✓	✓			S	S
AC-04(04)			✓			S	S

System-Specific Guidance:
For AC-04, the control of information flow within a system and between systems must be controlled. Information flow must be documented in the system SSPP. Controlling the flow of information between GSA systems and external systems using persistent connections is covered in interconnection security agreements specified in control CA-03, additional information is available in CIO-IT Security-06-30: Managing Enterprise Cybersecurity Risk and CIO-IT Security-24-125: Managing Information Exchange Agreements.

Docusign Envelope ID: 1636BF85-DA76-4F0E-964C-4C3DA19ABB87

Information flow control within a system and interconnected systems should be governed by the frameworks and services in the control parameter. Flow enforcement is also provided by the architectures of the systems and their networks, i.e., firewall rules, router policies, etc.

For AC-04(04), systems must employ mechanisms that preclude encrypted information from circumventing flow control mechanisms. For example, if all web traffic must be visible for inspection, encrypted web traffic must either be decrypted and inspected, blocked if decryption is not possible, terminating the connection.

3.5 AC-05 Separation of Duties

Control:

a. Identify and document [GSA SSO or Contractor recommended duties of individuals requiring separation, to be approved by the GSA CISO and AO];
b. Define system access authorizations to support separation of duties.

	Low	Mod	High	LATO	MiSaaS	Federal	Contractor
AC-05		✓	✓		✓	S	S

System-Specific Guidance:
For AC-05, the System Owner must ensure separation of duties which ensures that no single user has complete control over a single critical process (i.e., enough authorizations to perform fraudulent actions or inflict other damage). The roles and privileges for users are defined in the system's SSPP in Section 9.4, Types of Users. This section defines the authorized privileges (system access) based on functions performed, which supports separation of duties. The System Owner, ISSO, and ISSM sign the SSPP, effectively approving the separation of duties described therein. The CISO and AO approve the separation of duties when the authorization package is approved by issuing an ATO for the system.

3.6 AC-06 Least Privilege

Control: Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.

Control Enhancements:

(01) Least Privilege | Authorize Access to Security Functions. Authorize access for [any individual or role] to:
  (a) [GSA SSO or Contractor recommended security functions (deployed in hardware, software, and firmware) approved by the GSA CISO and AO]; and
  (b) [security-relevant information as approved by the GSA CISO and AO].

(02) Least Privilege | Non-Privileged Access for Non-Security Functions. Require that users of system accounts (or roles) with access to [all security functions (examples of security functions include but are not limited to: establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters, system programming, system and security administration, other privileged functions)], use non-privileged accounts or roles, when accessing non-security functions.

Docusign Envelope ID: 1636BF85-DA76-4F0E-964C-4C3DA19ABB87

(03) Least Privilege | Network Access to Privileged Commands. Authorize network access to [all privileged commands (i.e., any command requiring privileges above a standard user)] only for [GSA SSO or Contractor recommended compelling operational needs as approved by the GSA CISO and AO] and document the rationale for such access in the security plan for the system.

(05) Least Privilege | Privileged Accounts. Restrict privileged accounts on the system to [GSA SSO or Contractor recommended employees and contractors as approved by the GSA CISO and AO];

(07) Least Privilege | Review of User Privileges. FIPS 199 Moderate and High systems
(a) Review [annually as part of the annual account review (per AC-02j)] the privileges assigned to [all roles and users] to validate the need for such privileges; and
(b) Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs.

(09) Least Privilege | Log Use of Privileged Functions. Log the execution of privileged functions.

(10) Least Privilege | Prohibit Non-Privileged Users from Executing Privileged Functions. Prevent non-privileged users from executing privileged functions.

	Low	Mod	High	LATO	MiSaaS	Federal	Contractor
AC-06		✓	✓		✓	S	S
AC-06(01)		✓	✓			S	S
AC-06(02)		✓	✓		✓	S	S
AC-06(03)			✓			S	S
AC-06(05)		✓	✓	✓		S	S
AC-06(07)		✓	✓			S	S
AC-06(09)		✓	✓	✓	✓	S	S
AC-06(10)		✓	✓			S	S

System-Specific Guidance:
For AC-06, assigned authorizations must follow the concept of “least privilege,” limiting users to only those resources necessary to satisfy organizational mission/business needs. Granting permissions beyond this scope increases the attack surface of the system, allowing users to operate in unwanted ways. When additional privileges are granted, they should be in effect for the shortest duration necessary. Appendix E contains additional information on best practices regarding least privilege.

For AC-06(01), similar to the base AC-06 control, access to security functions should be identified in Section 9.4 of the SSPP and the approvals are based on approving the SSPP and the ATO of the system. Access to any security functions not addressed in Section 9.4 must be fully explained in the SSPP when AC-06(01) is addressed.

Security-relevant information includes, but is not limited to, filtering rules for routers or firewalls, configuration parameters for security services, cryptographic key management information, and access control lists. Authorized personnel include security administrators, system administrators, system security officers, system programmers, and other privileged users. Security-relevant functions include, but are not limited to, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited,

Docusign Envelope ID: 1636BF85-DA76-4F0E-964C-4C3DA19ABB87

and setting intrusion detection parameters, system programming, system and security administration, and other privileged functions.

For AC-06(02), privileged users/roles must use non-privileged accounts/roles when performing non-security functions.

For AC-06(03), systems must authorize network access to commands that require privileges above a standard user only when needed based on compelling operational needs of the system and its business function. The rationale for the network access to such privileges and the rationale for permitting such access must be described in the SSPP with approvals by the CISO and AO being provided when an ATO is signed based on an assessment of the control.

For AC-06(05), systems following the LATO process must provide privileged accounts (e.g., system administrator) only to those individuals approved by the GSA CISO and AO. The approval is granted by issuing an ATO based on an assessment that indicates this control has been met. In addition, as described in Appendix E, the level of investigation performed on an individual is based on the level of access that individual will need to a system.

For AC-06(07), the review of the account privileges assigned to all roles/users must be included in the annual review of accounts specified in control AC-02.j. This review is to validate existing privileges or to adjust privileges when they are no longer needed by the user or role.

For AC-06(09), systems must log the execution of privileged functions. Additional information regarding the auditing/logging of events for GSA systems is covered in CIO-IT Security-01-08.

For AC-06(10), systems must prevent non-privileged users from executing privileged functions. Effectively, this is accomplished by ensuring that non-privileged users, i.e., users that do not have a need to perform privileged functions based on their role or business need and/or users who do not have the required investigation for executing privileged functions are not granted them when they are assigned their account or role.

3.7 AC-07 Unsuccessful Logon Attempts

Control:

a. Enforce a limit of [not more than ten (10) failed access attempts] consecutive invalid logon attempts by a user during a [30-minute time period]; and
b. Automatically [lock the account/node for 30 minutes] when the maximum number of unsuccessful attempts is exceeded.

	Low	Mod	High	LATO	MiSaaS	Federal	Contractor
AC-07	✓	✓	✓			S	S

System-Specific Guidance:
All GSA systems must enforce a limit on unsuccessful access attempts (not more than 10 failed attempts within a 30-minute period) and lock the account/node for 30 minutes when the maximum number of unsuccessful attempts is exceeded.

Docusign Envelope ID: 1636BF85-DA76-4F0E-964C-4C3DA19ABB87

3.8 AC-08 System Use Notification

Control:

a. Display [a system use notification message or banner as defined in GSA CIO Order 2100.1)] to users before granting access to the system that provides privacy and security notices consistent with applicable Federal laws, Executive Orders, directives, regulations, policies, standards, and guidance and state that:
   1. Users are accessing a U.S. Government system;
   2. System usage may be monitored, recorded, and subject to audit;
   3. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and
   4. Use of the system indicates consent to monitoring and recording;

b. Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system; and

c. For publicly accessible systems:
   1. Display system use information [when accessed via logon interfaces with human users], before granting further access to the publicly accessible system;
   2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
   3. Include a description of the authorized uses of the system.

	Low	Mod	High	LATO	MiSaaS	Federal	Contractor
AC-08	✓	✓	✓		✓	S	S

System-Specific Guidance:

Publicly Accessible Systems

In accordance with Office of Management and Budget (OMB) M-23-22, for publicly accessible systems, rather than actively presenting a warning banner to users on GSA sites, those websites, systems, and applications may satisfy this control by linking to GSA.gov's Privacy and Security policies. Figure 8-1 is an acceptable method of linking to the policies. No additional System Use Notification is required. GSA's publicly accessible URLs are identified as 'External' in GSA's URL inventory.

Figure 8-1: Linking to Privacy and Security Policies Example

For instances where users register on a site, system use language should be presented with the terms and conditions for the user to agree to. Figure 8-2 is an example where users are presented the Rules of Use at account creation. This method satisfies the acknowledgement

Docusign Envelope ID: 1636BF85-DA76-4F0E-964C-4C3DA19ABB87

required from users that the system they are using will be subject to monitoring and they recognize that they are accessing a federal government system every subsequent time they login.

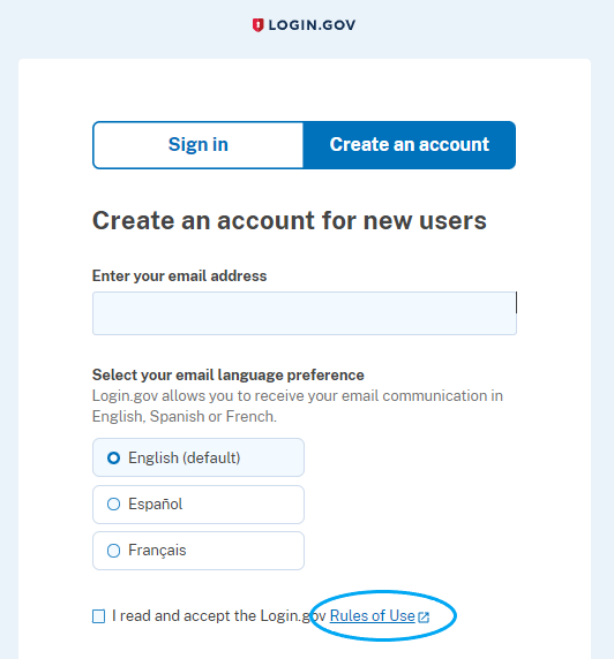

Figure 8-2: System Use Acknowledgement Example

Non-publicly Accessible Systems

All non-publicly accessible GSA systems must display the authorized GSA system use notification message (as provided in CIO 2100.1) before granting system access to persons. The system must require the person to acknowledge the system use notification before they can take additional actions on, or further access the system. Any System Use Notification message/banner that varies from GSA's approved banner must be documented in the systems SSPP and approved by the ISSM. For example, Contractor systems may have a banner that is worded differently, however all parts of the control must be addressed.

All GSA internal systems must display the authorized GSA system use notification message (as provided in CIO 2100.1) before granting system access. The system must require the user to acknowledge the system use notification before they can take additional actions on, or further access the system. The authorized use notification includes allowed adjustments for publicly accessible systems.

3.9 AC-10 Concurrent Session Control

Control: Limit the number of concurrent sessions for each [user] to [GSA SSO or Contractor recommended number to be approved by GSA CISO and AO].

	Low	Mod	High	LATO	MiSaaS	Federal	Contractor
AC-10			✓			S	S

Docusign Envelope ID: 1636BF85-DA76-4F0E-964C-4C3DA19ABB87

System-Specific Guidance:
For AC-10, each GSA system must limit the number of concurrent sessions for any user to a number that has been documented in the SSPP and approved by the GSA CISO and AO.

3.10 AC-11 Device Lock

Control:

a. Prevent further access to the system by [initiating a device lock after 15 minutes of inactivity; requiring the user to initiate a device lock before leaving the system unattended]; and
b. Retain the device lock until the user reestablishes access using established identification and authentication procedures.

Control Enhancements:

(01) Device Lock | Pattern-Hiding Displays. Conceal, via the device lock, information previously visible on the display with a publicly viewable image.

	Low	Mod	High	LATO	MiSaaS	Federal	Contractor
AC-11		✓	✓			S	S
AC-11(01)		✓	✓			S	S

System-Specific Guidance:
For AC-11, systems must automatically lock a user session after 15 minutes of inactivity. Users are required to initiate a device lock when stopping work and temporarily moving away from the immediate vicinity of the system. The user must reestablish access by providing appropriate identification and authentication before the device becomes unlocked. Device locks are temporary safeguards and not an acceptable substitute for logging out of a system.

For AC-11(01), systems' device locks must use a publicly viewable image (static or dynamic) to conceal the information visible on the display when the device was locked.

3.11 AC-12 Session Termination

Control: Automatically terminate a user session after [
(1) 30 minutes of inactivity
(2) the following timeframes, regardless of user activity:
    a. Thirty (30) days for systems at AAL1
    b. Twelve (12) hours for systems at AAL2 and AAL3.
Note: AAL2 and AAL3 require Two Factor Authentication].

	Low	Mod	High	LATO	MiSaaS	Federal	Contractor
AC-12		✓	✓		✓	S	S

System-Specific Guidance:
For AC-12, systems must terminate a user session after 30 minutes of inactivity. Authentication assurance levels (AALs) for systems are determined when a system completes a Digital Identity Acceptance Statement as part of its development and authorization processes. Systems at AAL1 must terminate user sessions after 30 days regardless of user activity, and at AAL2 and AAL3 after 12 hours.

Docusign Envelope ID: 1636BF85-DA76-4F0E-964C-4C3DA19ABB87

3.12 AC-14 Permitted Actions without Identification or Authentication

Control:

a. Identify [no user actions] that can be performed on the system without identification or authentication consistent with organizational mission and business functions; and
b. Document and provide supporting rationale in the security plan for the system, user actions not requiring identification or authentication.

	Low	Mod	High	LATO	MiSaaS	Federal	Contractor
AC-14	✓	✓	✓			S	S

System-Specific Guidance:
For AC-14, systems must prohibit any user action from being performed on the system without identification or authentication. Any public information on publicly available websites, such as GSA.gov may not require identification and authentication by users and therefore is available without specific user identification or authentication. Per AC-22 appropriate GSA individuals must decide whether specific data should be publicly accessible.

3.13 AC-17 Remote Access

Control:

a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and
b. Authorize each type of remote access to the system prior to allowing such connections.

Control Enhancements:

(01) Remote Access | Monitoring and Control. Employ automated mechanisms to monitor and control remote access methods.
(02) Remote Access | Protection of Confidentiality and Integrity Using Encryption. Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.
(03) Remote Access | Managed Access Control Points. Route remote accesses through managed network access control points.
(04) Remote Access | Privileged Commands and Access.
  (a) Authorize the execution of privileged commands and access to security-relevant information via remote access only in a format that provides assessable evidence and for the following needs: [GSA SSO or Contractor recommended and GSA CISO and AO approved special cases for remote administration and maintenance tasks]; and
  (b) Document the rationale for remote access in the security plan for the system.

	Low	Mod	High	LATO	MiSaaS	Federal	Contractor
AC-17	✓	✓	✓			S	S
AC-17(01)		✓	✓			S	S
AC-17(02)		✓	✓			S	S

Docusign Envelope ID: 1636BF85-DA76-4F0E-964C-4C3DA19ABB87

	Low	Mod	High	LATO	MiSaaS	Federal	Contractor
AC-17(03)		✓	✓			S	S
AC-17(04)		✓	✓			S	S

System-Specific Guidance:
For AC-17, GSA systems must control how remote access is allowed. Any method used to remotely access GSA systems must be approved by the System Owner under written authorization from the AO. Each type of approved remote access, such as via public Internet or VPN, must have documented parameters, including usage restrictions, configuration and connection requirements, and implementation guidance. Access must be authorized prior to allowing a remote connection. GSA internal and public web sites must implement Transport Layer Security (TLS) encryption as described in CIO-IT Security-14-69: SSL/TLS Implementation.

For AC-17(01), systems must use automated tools to monitor and control access methods to ensure compliance with GSA remote access policies.

For AC-17(02), systems must use cryptographic mechanisms (e.g., SSL/TLS, VPN tunnels, etc.) to protect the confidentiality and integrity of remote access sessions. Systems must protect the information from end-to-end.

For AC-17(03), systems must route remote access through GSA network access control points or network access control points which have been recommended by a GSA SSO or Contractor and approved by the GSA CISO and AO.

For AC-17(04), systems must limit the ability to execute privileged commands and access security-relevant information during remote access sessions only for special cases which have been approved by the GSA CISO and AO. Strictly limiting the execution of privileged commands and the ability to access security-relevant data helps reduce the organization's exposure and its susceptibility to adversarial threats via remote access capabilities. Any special use cases permitting access for these purposes must have the rationale documented in the systems' SSPP.

3.14 AC-18 Wireless Access

Control:

a. Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access; and
b. Authorize each type of wireless access to the system prior to allowing such connections.

Control Enhancements:

(01) Wireless Access | Authentication and Encryption. Protect wireless access to the system using authentication of [users and devices] and encryption;
(03) Wireless Access | Disable Wireless Networking. Disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment.
(04) Wireless Access | Restrict Configurations by Users. Identify and explicitly authorize users allowed to independently configure wireless networking capabilities.

Docusign Envelope ID: 1636BF85-DA76-4F0E-964C-4C3DA19ABB87

(05) Wireless Access | Antennas and Transmission Power Levels. Select radio antennas and calibrate transmission power levels to reduce the probability that signals can be received outside of organization-controlled boundaries.

	Low	Mod	High	LATO	MiSaaS	Federal	Contractor
AC-18	✓	✓	✓			S	S
AC-18(01)		✓	✓			S	S
AC-18(03)		✓	✓			S	S
AC-18(04)			✓			S	S
AC-18(05)			✓			S	S

System-Specific Guidance:
For AC-18, CIO 2100.1 and GSA's technical hardening guides specify configuration and connection requirements regarding wireless access. Except for normal web access (e.g., using a browser from a wireless device), systems must include in their SSPPs if wireless access is specifically designed for accessing system components. Any wireless access to a system must be considered as part of the system's architecture review and assessment, and would be authorized as part of the system's ATO.

In addition, GSA IT maintains two wireless networks: (1) a GSA Wireless Network, and (2) a GSA Guest Wireless Network that are configured to provide access to different user types and protect access to the GSA network. GSA IT scans for unauthorized wireless access points reports if any unauthorized access points are discovered. ISSOs and system/network administrators are responsible for controlling and monitoring wireless access to their systems/networks.

For AC-18(01), systems must authenticate users and devices and use cryptographic mechanisms to protect wireless system access. Additional requirements regarding the identification of users and devices are provided in CIO-IT Security-01-01 and CIO 2183.1.

For A-18(03), systems that will not utilize wireless access must disable wireless networking capabilities in system components before the components are issued and deployed in production.

For AC-18(04), systems must identify and explicitly authorize users permitted to independently configure wireless networking capabilities.

For AC-18(05), systems must reduce the probability that signals can be received outside of GSA-controlled boundaries by utilizing appropriate radio antennas and calibrating transmission power levels.

3.15 AC-19 Access Control for Mobile Devices

Control:

a. Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices to include when such devices are outside of controlled areas; and

Docusign Envelope ID: 1636BF85-DA76-4F0E-964C-4C3DA19ABB87

b. Authorize the connection of mobile devices to organizational systems.

Control Enhancements:

(05) Access Control for Mobile Devices | Full Device or Container-Based Encryption. Employ [at a minimum full device encryption, preferred container encryption] to protect the confidentiality and integrity of information on [GSA approved and authorized mobile devices].

	Low	Mod	High	LATO	MiSaaS	Federal	Contractor
AC-19	✓	✓	✓			H	H
AC-19(05)		✓	✓			C	C

Common Control Implementation:
For AC-19, CIO-IT Security-12-67: Securing Mobile Applications and Devices, establishes processes and procedures regarding usage restrictions, configuration and connection requirements, and implementation guidance for GSA-issued mobile devices, including smartphones and tablets and the applications loaded onto them. The GSA utilizes mobile device management technologies to authorize and control the use of GSA-issued mobile devices on GSA networks, including when these devices are outside of GSA-controlled areas.

For AC-19(05), the GSA enforces strong full-device encryption for GSA-issued mobile devices. Full-device encryption is enforced on mobile devices at all times. Containers in the context of this control are data structures such as files, records, or fields.

System-Specific Expectations:
For AC-19, AOs must authorize the connection of mobile applications on mobile devices to systems as part of the assessment and authorization process. ISSOs and system/network administrators are responsible for controlling and monitoring access to GSA systems by mobile applications on GSA devices. Additional guidance can be found in CIO-IT Security-12-67.

3.16 AC-20 Use of External Systems

Control:

a. [Establish terms and conditions per agreements established by CA-03; and identify controls asserted to be implemented on external systems per agreements established by CA-03], consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to:
   1. Access the system from external systems; and
   2. Process, store, or transmit organization-controlled information using external systems; or
b. Prohibit the use of [external systems not covered by an approved ISA/MOA or IEA/MOA per CA-03].

Control Enhancements:

(01) Use of External Systems | Limits on Authorized Use. Permit authorized individuals to use an external system to access the system or to process, store, or transmit organization-controlled information only after:

Docusign Envelope ID: 1636BF85-DA76-4F0E-964C-4C3DA19ABB87

(a) Verification of the implementation of controls on the external system as specified in the organization's information security and privacy policies and security and privacy plans; or
(b) Retention of approved system connection or processing agreements with the organizational entity hosting the external system.

(02) Use of External Systems | Portable Storage Devices – Restricted Use. Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems using [prohibits the use on any external system that is not GSA-owned including personally owned systems].

GSA Additional Guidance: Portable Storage Devices include digital media such as flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state, magnetic), compact discs, and digital versatile discs.

External systems are systems that are used by but not part of organizational systems, and for which the organization has no direct control over the implementation of required controls or the assessment of control effectiveness. External systems include personally owned systems, components, or devices; privately owned computing and communications devices in commercial or public facilities; systems owned or controlled by nonfederal organizations; systems managed by contractors; and federal information systems that are not owned by, operated by, or under the direct supervision or authority of the organization. External systems also include systems owned or operated by other components within the same organization and systems within the organization with different authorization boundaries.

	Low	Mod	High	LATO	MiSaaS	Federal	Contractor
AC-20	✓	✓	✓			S	S
AC-20(01)		✓	✓			S	S
AC-20(02)		✓	✓			C	C

Common Control Implementation:
For AC-20(02), GSA Order CIO 2100.1, "GSA Information Technology(IT) Security Policy" prohibits the use of GSA-provided portable storage devices (e.g., USB flash drives, SD cards, etc.) on external systems (e.g., personal computers, any external system that is not GSA-owned). All portable storage devices must be encrypted with a Federal Information Processing Standard 140-3[1]/140-02, "Security Requirements for Cryptographic Modules" validated encryption module.

System-Specific Expectations:
For AC-20, systems must prepare and have approved Interconnection Security Agreements(ISA)/Memorandum of Agreements (MOA) or Information Exchange Agreements (IEA)/MOAs documenting the terms and conditions and control assertions regarding external systems. CIO 2100.1, CIO-IT Security-06-30, and CIO-IT Security-24-125: Managing Information Exchange Agreements identify the types of agreements required when using external systems.

[1] NIST has issued FIPS 140-3 and no longer accepts FIPS 140-2 modules for validation. However, previously validated 140-2 modules will be accepted through September 22, 2026. For additional information see the NIST cryptographic module validation program web page.

Docusign Envelope ID: 1636BF85-DA76-4F0E-964C-4C3DA19ABB87

The use of external systems not covered by an ISA/MOA or IEA/MOA is prohibited per CIO 2100.1, CIO-IT Security-06-30, and CIO-IT Security-24-125.

For AC-20(01), systems must verify adequate security controls are in place to use an external information system via an ISA/MOA or IEA/MOA per CIO 2100.1, CIO-IT Security-06-30, and CIO-IT Security-24-125.

Systems must have a signed ISA/MOA or IEA/MOA approved by the GSA and the external system's organization in order to use an external information system per CIO 2100.1, CIO-IT Security-06-30, and CIO-IT Security-24-125. The ISA/MOA or IEA/MOA must be included in the A&A package for the GSA system.

For AC-20(02), none, common control.

3.17 AC-21 Information Sharing

Control:

a. Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions for [GSA SSO or Contractor recommended information sharing circumstances where user discretion is required to be approved by the GSA CISO and AO]; and
b. Employ [GSA SSO or Contractor recommended automated mechanisms or manual processes to be approved by the GSA CISO and AO] to assist users in making information sharing and collaboration decisions.

	Low	Mod	High	LATO	MiSaaS	Federal	Contractor
AC-21		✓	✓		✓	S	S

System-Specific Expectations:
For AC-21, the GSA CISO and the AO must approve the sharing of sensitive data and information (e.g., privileged or proprietary information, PII) based on the sharing partner's access authorizations. GSA systems must utilize automated tools or, in some cases, manual processes to help system users make decisions about information sharing and collaboration.

The following GSA Orders govern the sharing of information with partners and the public:

- GSA Order CIO 2103.2, "Controlled Unclassified Information (CUI) Policy;"
- GSA Order CIO 2142.1, "CHGE 1, GSA Information and Data Quality Handbook;"
- GSA Order CIO 2164.2, "Internal Clearance Process for GSA Data Assets;" and
- GSA Order CIO 2231.1, "GSA Data Release Policy."

3.18 AC-22 Publicly Accessible Content

Control:

a. Designate individuals authorized to make information publicly accessible;
b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information;

Docusign Envelope ID: 1636BF85-DA76-4F0E-964C-4C3DA19ABB87

c. Review the proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included; and
d. Review the content on the publicly accessible system for nonpublic information [quarterly] and remove such information, if discovered.

	Low	Mod	High	LATO	MiSaaS	Federal	Contractor
AC-22	✓	✓	✓			S	S

System-Specific Expectations:
For AC-22, individuals must be designated and trained on making information publicly available. The information must be reviewed before it is made publicly available. Publicly available information is to be reviewed quarterly and any information that should be nonpublic must be removed.

For details on GSA's processes for identifying and clearing data or information publicly accessible refer to the following GSA Orders:

- CIO 2142.1, "CHGE 1, GSA Information and Data Quality Handbook;"
- CIO 2164.2, "Internal Clearance Process for GSA Data Assets;" and
- CIO 2231.1, "GSA Data Release Policy."

Docusign Envelope ID: 1636BF85-DA76-4F0E-964C-4C3DA19ABB87

Appendix A: CSF Categories/Subcategories

The CSF focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes. The core of the CSF consists of five concurrent and continuous Functions—Identify (ID), Protect (PR), Detect (DE), Respond (RS), and Recover (RC). The CSF complements, and does not replace, an organization's risk management process and cybersecurity program. The GSA uses NIST's RMF as its primary risk management process. Table A-1 lists the Categories and Subcategories from the CSF that are identified as related to the implementation of policies, procedures, and processes implementing the NIST SP 800-53, Revision 5 AC controls. CIO 2100.1 and this procedural guide provide GSA's policies and procedural guidance regarding access control to GSA systems and implementing AC controls.

Table A-1: CSF Categories/Subcategories and the AC Control Family

CSF Category/ Subcategory Identifier	Definition/Description
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-3:** Organizational communication and data flows are mapped (AC-04). **ID.AM-4:** External information systems are catalogued (AC-20).
Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational cybersecurity policy is established and communicated (AC-01). **ID.GV-3:** Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed (AC-01).
Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-3:** Remote access is managed (AC-01, AC-17, AC-19, AC-20). **PR.AC-4:** Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties (AC-01, AC-02, AC-03, AC-05, AC-06, AC-14). **PR.AC-5:** Network integrity is protected (e.g., network segregation, network segmentation) (AC-04, AC-10). **PR.AC-7:** Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks) (AC-14).
Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-5:** Protections against data leaks are implemented (AC-04, AC-05, AC-06).

Docusign Envelope ID: 1636BF85-DA76-4F0E-964C-4C3DA19ABB87

CSF Category/ Subcategory Identifier	Definition/Description
Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-8:** Effectiveness of protection technologies is shared (AC-21).
Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-3:** The principle of least functionality is incorporated by configuring systems to provide only essential capabilities (AC-03). **PR.PT-4:** Communications and control networks are protected (AC-12, AC-17, AC-18).
Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed (AC-04).
Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-3:** Personnel activity is monitored to detect potential cybersecurity events (AC-02).

Docusign Envelope ID: 1636BF85-DA76-4F0E-964C-4C3DA19ABB87

Appendix B: Policy

The following extracts from CIO 2100.1 contain information related to the implementation of access control for GSA IT systems and data.

Chapter 3: Policy for Identify states:

1. Asset Management.

c. CIO-IT Security-24-125 provides guidance on information exchanges and the types of agreements based on the level and type of data exchanged, the type or method of exchange, and if the exchange is between GSA systems (internal) or between GSA and another entity's systems (external). All communications and data flows and system interconnections, both internal and external, for an information system must be documented in the System Security and Privacy Plan (SSPP). All information exchanges and agreements must be reviewed and certified or updated on the specified timeframe within the agreement (typically annually).

Chapter 4: Policy for Protection states:

1. Identity Management, Authentication and Access Control.

i. Non-person entities (NPE) must be managed for all systems, including establishing, activating, modifying, reviewing, disabling, and removing accounts. Reviews and validations of all accounts shall be completed consistent with the SSPP to ensure the continued need for system access.

j. Information system user accounts (i.e., persons) must be managed for all systems, including establishing, activating, modifying, reviewing, disabling, and removing user accounts. Reviews and validations of all user accounts shall be completed consistent with the SSPP to ensure the continued need for system access. GSA user account management processes include:

(1) Supervisors, CORs, or account managers coordinating and arranging system access termination for all departing or resigning personnel, including both GSA employees and contractors.

(2) Supervisors, CORs, or account managers initiating account removal, disablement, or permission changes based on a review of information provided by the OCISO (e.g., separation lists, role revisions) for GSA users, including both GSA employees and contractors.

(3) System Owners/account managers verifying that separated GSA users, i.e., users with an ENT account, no longer maintain access to GSA IT systems or resources after 30 days of separation. Verification of non-GSA users' access removal must be performed within the time period specified in the SSPP in NIST control AC-2(3).

(4) ISSOs, ISSMs, and System Owners ensuring processes for removing or modifying access to GSA systems, based on terminations and transfers, are performed IAW procedures specified in GSA CIO-IT Security-03-23.

(5) Supervisors, CORs, or System/Data Owners submitting GSA user access requests and user permission or role changes for account manager approval based on a user's job function and need-to-know.

(6) System Owners/Data Owners, with assistance from the designated ISSO, ensuring system access is restricted to authorized users who meet GSA and system access requirements, are familiar with internal security practices, and have completed requisite security and privacy awareness training programs.

Docusign Envelope ID: 1636BF85-DA76-4F0E-964C-4C3DA19ABB87

(7) System Owners/Data Owners, with assistance from the designated ISSO, ensuring system access authorizations enforce separation of duties, see Separation of duties.

j. Data or System Owners only grant access to the information system based on a valid need-to-know/need-to-share determined during the account authorization process and the intended system usage.

k. A user account that has been or is expected to be idle for an extensive period of time consistent with account abandonment must be disabled.

l. To securely share files in Google Drive/Google Sites with other government customers and business partners who do not use Google in their workplace, a GSA Affiliated Customer Account (GACA) must be created by the external non-GSA user. GSA employees, contractors, or other users (e.g., detailees, interns) requiring regular/repeated access to the GSA network to conduct business are not permitted to use GACA accounts.

m. System/network administrators must have separate administrator and user accounts, if applicable (e.g., Microsoft Windows accounts). The administrator privileged account must only be used when administrator rights are required to perform a job function. A normal user account should be used at all other times.

s. Remote access connections, sessions, and timeout/termination parameters must meet the requirements specified in the procedural guides listed in Section 1 of this Chapter.

t. FIPS 199 Moderate and High systems must terminate user sessions regardless of user activity:

(1) After 30 minutes of inactivity.

(2) Thirty days for systems at AAL1.

(3) Twelve hours for systems at AAL2 and AAL3.

u. An AO, upon concurrence of the GSA CISO, may grant a deviation to individual requirements specified in the guides only if the system is technically unable to implement the requirement or there is an approved business justification and sufficient compensating controls have been implemented to reduce the risk to an acceptable level. See Chapter 1, Section 5, Compliance and Deviations.

v. Remote access/endpoint security.

(1) All desktop or laptop computers, including personal devices, connecting remotely to GSA must have anti-virus software running with the latest signature files, a firewall installed and running, and all security patches installed. Failure to have current security signatures or patches may result in loss of access to the GSA network or data.

(2) All computers accessing GSA through a GSA Secure Sockets Layer (SSL) or Internet Protocol Security (IPsec) Virtual Private Network (VPN) must allow an endpoint device with the ability to check for the presence of a client firewall, up-to-date virus protection software and up-to-date patches. The endpoint device must also verify the absence of malicious software (e.g., Trojans, worms, malware, spyware, etc.) on the client machine. Machines failing this scan will not be allowed access to the GSA network or any GSA IT resources.

(3) Only properly secured GSA GFE (based on the scans noted above) will be allowed unrestricted remote access to the GSA network.

(4) Personal computers and/or contractor computers will only be allowed access to the Citrix NetScaler and will not have the ability to map local drives (contingent on passing the scans noted above). No PII or other data deemed sensitive by the data owner shall be stored on non-GFE.

(5) In special cases for remote administration and maintenance tasks, contractors will be allowed restricted IPsec access to specific GSA IP addresses (contingent on passing the scans noted above).

w. Remote access to the GSA domain must be restricted to secure methods using approved identification and authentication methods to provide detection of intrusion attempts and protection against unauthorized access.

Docusign Envelope ID: 1636BF85-DA76-4F0E-964C-4C3DA19ABB87

(1) Only GSA employees and contractor personnel are permitted to use GSA furnished computers, a GSA VPN connection, a Zscaler Private Access connection, or a GSA provided or funded internet connection.

(2) Connections to other networks or computers (split tunneling) are not permitted when connected to the GSA network. However, accessing GSA's network unless approved by GSA's CISO. However, accessing GSA's network via the GSA-provided VPN software over a network is allowed.

(3) When using the GSA IT IPsec VPN or Zscaler Private Access, users must connect using only IP and must have the client firewall bound to all network adapters.

aa. All GSA systems must implement logical access controls to authorize or restrict the activities of users and system personnel to authorized transactions and functions IAW GSA CIO-IT Security-01-07.

bb. Privileged rights including but not limited to "administrator," "root," and "power user" shall be restricted to authorized employees and contractors as approved by the AO.

cc. Information systems must enforce 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.

dd. User authorizations must be verified annually for all information systems to determine if they remain appropriate.

ee. Systems requiring users to maintain an active email account must suspend or revoke access for users whose email credentials are no longer valid.

ff. Separation of duties. The following requirements apply to FIPS 199 Moderate and High systems only.

(1) Any access or permissions clearly violating established separation of duties policies must be coordinated with the designated SSO and ISSM/ISSO to correct or resolve conflicting role assignments.

(2) Shared user accounts violate the principles of separation of duties and non-repudiation and must be detected and removed when discovered.

(3) The delegation of user roles or permissions for applications, in particular those containing PII and/or other CUI, must be compliant with the principles of least privilege, separation of duties, and need-to-know.

(4) Responsibilities with a security impact must be shared among multiple staff by enforcing the concept of separation of duties, which requires that individuals do not have control of the entirety of a critical process. Define and implement detailed separation of duties policies for IT systems based on the specific processes, roles, permissions, and responsibilities of personnel involved in departmental business operations.

(5) Every SSO including Regional Offices, must consider how a separation of duties conflict can arise from shared access to applications and systems. Specifically, application programmers and configuration management personnel should not generally have concurrent access to the development and production environment. Failure to segregate access to source code and production code increases the risk of unauthorized modifications to programs being implemented into production systems, introducing vulnerabilities, and negatively impacting the integrity and availability of data generated and stored in the system.

(6) User account privileges must be reviewed across the appropriate Service and Staff Office application portfolio to assess incompatible and non-compliant role assignments (e.g., review of user access assignments across multiple significant systems sharing data or passing transactions to identify conflicts with separation of duties policy).

(7) Job descriptions and roles must be documented to accurately reflect the assigned duties, responsibilities, and separation of duties principles. By clearly documenting position responsibilities and functions, employees are positioned to better execute their duties IAW policy.

Docusign Envelope ID: 1636BF85-DA76-4F0E-964C-4C3DA19ABB87

(8) Formal procedures must be established to guide personnel in performing their duties, with identification of prohibited actions violating separation of duties.

(9) Duties shall be segregated among users, ensuring the following functions shall not generally be performed by a single individual:

(a) Data entry and verification of data. Any data entry or input process requiring a staff member to inspect, review, audit, or test the input to determine that the input meets certain requirements should not permit the same individual to both enter and verify the data. The objective is to eliminate self-certification or verification of data input or entry procedures. Note that this could be an automated or manual process and is not limited to financial transactions.

(b) Data entry and its reconciliation to output. Any data entry or input process requiring reconciliation or matching of transactions to identify discrepancies should not permit the same individual to both enter and reconcile data.

(c) Input of transactions for incompatible processing functions (e.g., input of vendor invoices and purchasing and receiving information).

(d) Data entry and supervisory authorization functions (e.g., authorizing a rejected transaction to continue processing exceeding some limit requiring a supervisor's review and approval).

(10) A system leveraging an agile development methodology in a DevSecOps environment must follow separation-of-duties best security practices IAW CIO-IT Security-19-102, DevSecOps Program OCISO.

(11) Proper separation of duties must be ensured for GSA IT system maintenance, management, and development processes.

(12) Information systems must enforce separation of duties through assigned access authorizations.

(13) Since critical processes can span separate and distinct applications and systems, all SSOs including Regional Offices will take a macro view of existing roles to define and establish incompatibilities and separation of duties conflicts across an entire business process. This means examining roles spanning multiple IT systems or applications to uncover conflicts not immediately apparent (e.g., an individual has permissions to create and/or modify vendor data in a General Ledger system and the ability to create invoices and purchase orders in an Accounts Payable system).

(14) All SSOs including Regional Offices must establish physical and logical access controls to enforce separation of duties policy and alignment with organizational and individual job responsibilities.

(15) Annual assessments must review the effectiveness of control techniques, with an emphasis on activities unable to be controlled through logical, physical, or compensating controls. The reviews determine whether in-place control techniques are maintaining risks within acceptable levels (e.g., periodic risk assessments).

gg. All GSA workstations and mobile devices shall initiate a device lock after 15 minutes of inactivity. The device lock shall remain in effect until the user re-establishes access using appropriate identification and authentication.

hh. OAuth 2.0 is an industry standard protocol approved by GSA. It enables a gsa.gov user to grant access to their account or data in Google Apps to a relying party. It is used in a wide variety of services for user authentication. The following policies apply to the use of OAuth 2.0.

(1) GSA IT's OCISO shall monitor and restrict the integration of gsa.gov accounts with OAuth 2.0 to third-party services including but not limited to; websites, Software as a Service (SaaS), mobile applications, and Google Apps Scripts.

(2) Use of the Auth 2.0 Access Scopes listed below is prohibited unless integrated with websites, mobile apps, and SaaS authorized to operate by GSA and/or included in the GSA IT Standards Profile.

Docusign Envelope ID: 1636BF85-DA76-4F0E-964C-4C3DA19ABB87

(a) Access Inbox and Contacts Information. Allows view of email messages and settings.

(b) Access Personal Information. Allows management of user calendars.

(c) Act on Behalf of User. Allows view and modify but not deletion of user email.

(d) Full Data Access. Allows view and manage of files and documents in connecting users Google Drive.

(e) Limited Access to Data and Files. Can be varied from access to a single file to allowing the app to view and manage its own configuration data in Google Drive.

(f) Manage Devices. Administrator's scope to view and manage mobile devices' metadata.

(g) Manage User Activity. Administrator's scope to view users on a domain; manage org units in a domain; view org units in a domain; view and manage provisioning of users in a domain; general domain Application Program Interface (API) operations include managing a domain's language, organization name, max number of users; current number of users.

(h) Other. Miscellaneous permissions. Restrictions are detailed in the system authorization letter.

(i) Payment Information. Read Google Wallet credentials from the production environment.

(j) Read-only Access to Data and Files. “Read-only Access” to data and files.

(k) Access Location Information. Google Map Data API - View Google Maps engine data; Google FIT: Location.

(3) The OAuth 2.0 Access Scopes listed below are authorized for integration with gsa.gov accounts with no restriction.

(a) Basic Info. View an email address; View basic information about an account, including name, public profile URL, photo, gender, birthdate, country, language, and time zone.

(b) Limited access to data and Files. Access Google+ features which are generally public.

(c) Other access scopes similar to those in (a) and (b) above that provide access to publicly available information and do not conflict with prohibited access scopes.

ii. Google Apps Script is a JavaScript cloud scripting language that facilitates the automation of routine tasks across Google Apps and third-party services. All scripts are subject to GSA IT review to verify author; access scope; where the script resides (e.g., internal vs external); type of data accessed; and storage of accessed data.

(1) Internally developed scripts are implicitly allowed but require review by the OCISO and may be restricted from use pending the results of the OCISO review.

(2) Internally developed scripts shall follow the GSA naming convention. “GSA” immediately followed by an underscore “_” or single dash “-,” a 1 to 5 character SSO official symbol designation of the script’s author, immediately followed by an underscore “_” or single dash “-”, and followed by a descriptive script name (e.g., “GSA_IS_Script Name”).

(3) Externally developed scripts are prohibited but may be allowed following OCISO review and approval.

mm. Non-GFE cannot access the GSA internal wireless network in Regional and Central Office Buildings; they can connect only to the GSA Guest Wireless Network to access the Internet and GSA resources available to the public (www.gsa.gov).

(1) Guest wireless accounts are not ENT accounts.

(2) Guest wireless traffic will be subject to the same content filtering as traffic on the production network.

nn. All non-GFE/workstations connected to the GSA Wired Network shall only be allowed access to the Internet (i.e., guest network only, no access allowed to the GSA resources).

Docusign Envelope ID: 1636BF85-DA76-4F0E-964C-4C3DA19ABB87

tt. All GSA systems must incorporate a proper user identification and authentication methodology. Refer to the GSA CIO-IT Security-01-01 for additional details.

3. Accessing GSA Resources.

a. GSA enterprise users must read and acknowledge GSA Order CIO 2104.1B CHGE 2, GSA IT General Rules of Behavior, within 90 days of being granted access to the enterprise, and annually thereafter.

c. Users have no expectation of privacy on GSA IT systems. All activity on GSA IT systems is subject to monitoring and internal GSA IT systems must display an approved warning banner to all users indicating the system is subject to monitoring. The following warning banner must be based on these instructions:

(1) Paragraph two of the warning banner is only required if the system contains CUI;

(2) Paragraph three is optional but is a best practice.

(3) For publicly accessible sites (i.e., open to the Internet), the sentence “Therefore no expectation of privacy is to be assumed” shall be removed.

**********WARNING**********

This is a U.S. General Services Administration Federal Government computer system that is "FOR OFFICIAL USE ONLY." This system is subject to monitoring. Therefore, no expectation of privacy is to be assumed. Individuals found performing unauthorized activities may be subject to disciplinary action including criminal prosecution.

This system contains Controlled Unclassified Information (CUI). All individuals viewing, reproducing or disposing of this information are required to protect it in accordance with 32 CFR Part 2002 and GSA Order CIO 2103.2 CUI Policy.

For additional information: [contact information or website where users can get help].

****

4. Data Security

a. All sensitive data (to include PII/CUI and PCI data; authenticators including but not limited to passwords, tokens, keys, certificates, and hashes; and business sensitive data as determined by the AO) must be encrypted everywhere (i.e., at file level, database level, at rest, and in transit). Encryption algorithms and modules must be FIPS 140-3/140-2 validated.

(1) For databases, encryption of the whole database, table, column, or field levels is acceptable, as appropriate. Other methods including but not limited to application encryption or tokenization is also acceptable.

(2) For web services connections, implement end-to-end encryption terminating the connection at the web server; connections terminated at a load balancer shall employ re-encryption techniques to ensure end-to-end encryption.

(3) Internet accessible Websites shall implement HTTPS Only with HTTP Strict Transport Security (HSTS), have no weak ciphers, have no weak protocols, and preload .gov domains.

(4) Systems implementing encryption must follow the key management procedures and processes documented in GSA CIO-IT Security-09-43: Key Management.

(5) Web sites (internal and public) with authentication functions, must implement Transport Layer Security (TLS) encryption with a FIPS 140-3/140-2 validated encryption

Docusign Envelope ID: 1636BF85-DA76-4F0E-964C-4C3DA19ABB87

module. SSL/TLS implementation must be IAW GSA CIO-IT Security-14-69, SSL/TLS Implementation Guide.

b. Sensitive data shall not be transferred to or accessed from non GSA systems.

c. Authorization to sensitive data must occur at the point of access (Application, API, Database, File)

d. Remote access to sensitive data may occur only via GFE or through an approved GSA virtual interface (i.e., Citrix and/or VDI).

e. PII/CUI stored on network drives and/or in application databases must have proper access controls (i.e., user identification, authentication, and authorization) and shall be made available only to those individuals with a lawful government purpose.

7. Protective technology

j. Information systems must run with the least amount of system privilege needed to perform a specific function and support system access granted on a need-to-know basis.

k. Information systems must be configured to the most restrictive mode (e.g., limiting ports, protocols, services, etc.) consistent with operational requirements.

p. If GSA systems interconnect, they must connect using a secure methodology providing security commensurate with the acceptable level of risk as defined in the system security plan and limiting access only to the information needed by the other system IAW GSA CIO-IT Security-01-07 and GSA CIO-IT Security-06-30.

Chapter 5: Policy for Detect Function states:

3. Security Continuous Monitoring

n. For contractors and outsourced operations, implement appropriate safeguards to monitor GSA information and information systems for unauthorized access throughout all phases of a contract. Review contracts to ensure information security is appropriately addressed in the contracting language. GSA CIO-IT Security-09-48 establishes the language for GSA IT acquisitions contracts. All applicable NIST SP 800-53, Revision 5 controls should be put on contract (and a reasonable subset continuously monitored using guidance provided by the OCISO) for all contractor and outsourced operations. Given that the GSA IT security program is risk-based, the System Owner/program manager and ISSO can make risk-based decisions on tailoring the system’s baseline security controls and then obtain concurrence from the AO and the CISO. Any controls tailored out of the baseline must have the rationale for the decision documented in the system’s SSPP.

Docusign Envelope ID: 1636BF85-DA76-4F0E-964C-4C3DA19ABB87

Appendix C: References

Federal Laws, Standards, Regulations, and Publications:

- EO 13800, Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
- FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems
- NIST Cybersecurity Framework, Framework for Improving Critical Infrastructure Cybersecurity
- NIST SP 800-37, Revision 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
- NIST SP 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations
- OMB M-23-22, Delivering a Digital-First Public Experience

GSA Policies, Procedures, Guidance:

The GSA policies listed below are available on the GSA.gov Directives Library page. The GSA CIO-IT Security Procedural Guides listed below are available on the GSA.gov IT Security Procedural Guides page with the exception of CIO-IT Security-18-90 and CIO-IT Security-12-67 which are restricted. It is available on the internal GSA InSite IT Security Procedural Guides page.

- GSA Order CIO 2100.1Q, GSA Information Technology (IT) Security Policy
- GSA Order CIO 2103.2, Controlled Unclassified Information (CUI) Policy
- GSA Order CIO 2104.1C, GSA Information Technology (IT) General Rules of Behavior (ROB)
- GSA Order CIO 2142.1P, CHGE 1, GSA Information and Data Quality Handbook
- GSA Order CIO 2164.2A, Internal Clearance Process for GSA Data Assets
- GSA Order CIO 2183.1, Enterprise Identity, Credential, and Access Management (ICAM) Policy
- GSA Order CIO 2231.1, GSA Data Release Policy
- CIO-IT Security-01-01: Identification and Authentication (I&A)
- CIO-IT Security-03-23: Termination and Transfer
- CIO-IT Security-01-08: Audit and Accountability (AU)
- CIO-IT Security-06-30: Managing Enterprise Cybersecurity Risk
- CIO-IT Security 06-32: Media Protection
- CIO-IT Security-09-44: Plan of Action and Milestones (POA&M)
- CIO-IT Security-09-48: Security and Privacy Requirements for IT Acquisition Efforts
- CIO-IT Security-12-64: Physical and Environmental Protection (PE)
- CIO-IT Security-12-67: Securing Mobile Applications and Devices
- CIO-IT Security-14-69: SSL/TLS Implementation
- CIO-IT Security-18-90: Common Control Catalog (CCC)
- CIO-IT Security-24-125: Managing Information Exchange Agreements

Docusign Envelope ID: 1636BF85-DA76-4F0E-964C-4C3DA19ABB87

Appendix D: Roles and Responsibilities

There are many roles associated with implementing an effective access control program. The roles and responsibilities provided in this appendix have been extracted or paraphrased from GSA Order CIO 2100.1 or summarized from GSA and Federal guidance. Complete roles and responsibilities for agency management officials and roles with significant IT Security responsibilities are defined in CIO 2100.1.

Authorizing Officials (AOs)

Responsibilities include the following:

- Implementing detailed separation of duties policies for IT systems based on the specific processes, roles, permissions, and responsibilities of personnel involved in GSA business operations;
- Establishing physical and logical access controls to enforce separation of duties policies and alignment with organizational and individual job responsibilities;
- Ensuring that GSA information systems under their purview have implemented the required AC controls in accordance with GSA and Federal policies and requirements.

Information Systems Security Managers (ISSMs)

Responsibilities include the following:

- Coordinating with ISSOs to establish and manage processes and procedures supporting AC controls for all systems under their purview;
- Coordinating with the AO, System Owner, ISSOs, and OCISO directors, as necessary, regarding AC control implementation and compliance with NIST and GSA requirements;
- Working with the ISSO and System Owner to develop, implement, and manage a Plan of Action and Milestones (POA&M) for their respective systems IAW GSA CIO-IT Security-09-44.

Information Systems Security Officers (ISSOs)

Responsibilities include the following:

- Ensuring necessary AC security controls are in place and operating as intended;
- Developing POA&Ms in collaboration with ISSMs, System Owners, and other system personnel, when necessary, for systems under their purview IAW CIO-IT Security 09-44;
- Ensuring the access control mechanisms, processes, and procedures in their assigned systems are administered and operating as intended, including reviewing system role assignments to validate compliance with principles of least privilege.

System Owners

Responsibilities include the following:

- Ensuring necessary AC security controls are in place and operating as intended;
- Conducting annual reviews and validation of system users' accounts to ensure the continued need for access to a system and verify users' authorizations (rights/privileges);

Docusign Envelope ID: 1636BF85-DA76-4F0E-964C-4C3DA19ABB87

- Defining, implementing, and enforcing detailed separation of duties by ensuring single individuals do not have control of the entirety of a critical process, roles, permissions, and/or responsibilities.
- Coordinating with IT security personnel, including the ISSM and ISSO and Data Owners, to ensure implementation of system and data security requirements;
- Working with the ISSO and ISSM to develop, implement, and manage POA&Ms for their system IAW CIO-IT Security 09-44;
- Working with the data owner, granting access to the information system based on a valid need-to-know/need-to-share that is determined during the account authorization process and the intended system usage.

Data Owners

Responsibilities include the following:

- Working with the System Owner, with assistance from the ISSO, to ensure access is restricted to authorized users that have completed required background investigations, are familiar with internal security practices, and have completed requisite security awareness training programs (e.g., the annual IT Security Awareness Training and Sharing Information in a Collaborative Environment training);
- Reviewing access authorization listings and determining whether they remain appropriate at least annually;
- Ensuring that data is not processed on a system with security controls that are not commensurate with the sensitivity of the data;
- Coordinating with IT security personnel including the ISSM and ISSO and System Owners to ensure implementation of system and data security requirements.

Contracting Officers (COs)/Contracting Officer Representatives (CORs)

Responsibilities include the following:

- Coordinating with the CISO or other appropriate official as required ensuring that all agency contracts and procurements are compliant with the agency's information security policy, and include appropriate security contracting language and security requirements in each contract and task order;
- Identifying, initiating, and adhering to favorable enter on duty (EOD) requirements for contractor background investigations in collaboration with the GSA Personnel Security Officer/Office of Mission Assurance;
- Ensuring new solicitations for all GSA IT systems include the security contract language from GSA CIO-IT Security-09-48: Security and Privacy Requirements for IT Acquisition Efforts.

Custodians

Responsibilities include the following:

- Coordinating with Data Owners and System Owners to ensure the data is properly stored, maintained, and protected;
- Accessing data only on a need-to-know basis as determined by the data owner.

Docusign Envelope ID: 1636BF85-DA76-4F0E-964C-4C3DA19ABB87

Authorized Users of IT Resources

Responsibilities include the following:

- Familiarizing themselves with any special requirements for accessing, protecting, and using data, including Privacy Act requirements, copyright requirements, and procurement-sensitive data;
- Ensuring that adequate protection is maintained on their workstation, including not sharing passwords with any other person and logging out, locking, or enabling a password protected screen saver, and removing their PIV card before leaving their workstation;
- Utilizing assigned privileged access rights (e.g., administrator, power user, database administrator, web site administrator, etc.) to a computer based on need-to-use (i.e., using accounts with those privileges only when the privileges are required to complete an action);
- Ensuring personally identifiable information (PII) and/or sensitive data stored on any workstations or mobile devices including, but not limited to, laptop computers, notebook computers, external hard drives, USB drives, CD-ROMs/DVDs, and personal digital assistants is encrypted with GSA provided encryption;
- Ensuring PII and/or sensitive data is only accessed remotely from Government Furnished Equipment (GFE) or through an approved GSA virtual interface (i.e., Citrix and/or VDI). Note: Remote access is permitted unless a system's AO or SAOP explicitly prohibit such access.

GSA Personnel Security Officer/Office of Mission Assurance

Responsibilities include the following:

- Developing and implementing access agreements, and personnel screening, termination, and transfer procedures;
- Ensuring consistent and appropriate sanctions for personnel violating management, operation, or technical information security controls.

System/Network Administrators

Responsibilities include the following:

- Ensuring the appropriate security requirements (including access controls) are implemented consistent with GSA IT security policies and hardening guidelines;
- Utilizing privileged access rights (e.g., "administrator," "root," etc.) to a computer based on a need-to-use basis (i.e., using accounts with those privileges only when the privileges are required to complete an action);
- Ensuring system/network administrators have separate administrator and user accounts, if applicable (e.g., Microsoft Windows accounts). A normal user account should be used unless administrator rights are required to perform a job function;
- Creating, modifying, and deleting accounts, access rights/privileges, and roles in cooperation with the System Owner, data owner, and ISSM/ISSO.

Docusign Envelope ID: 1636BF85-DA76-4F0E-964C-4C3DA19ABB87

Supervisors

Responsibilities include the following:

- Conducting annual review and validation of staff user accounts to ensure the continued need for access to a system;
- Coordinating and arranging system access requests for all new or transferring employees and verifying an individual's need-to-know (authorization);
- Coordinating and arranging system access termination for all terminating or transferring personnel;
- Coordinating and arranging system access modifications for personnel;
- Documenting job descriptions and roles to accurately reflect the assigned duties, responsibilities, and separation of duties principles. Establishing formal procedures to guide personnel in performing their duties, with identification of prohibited actions.

Docusign Envelope ID: 1636BF85-DA76-4F0E-964C-4C3DA19ABB87

Appendix E: Access Controls Best Practices

Access controls are categorized as preventive controls. Preventive controls are proactive and used to deter unauthorized access to IT resources. Controlling logon/logoff to an information system and verifying whether an individual is authorized specific types of access to the system and its data a preventive control. Detective controls, on the other hand, are reactive and warn personnel of violations or attempted violations when or after they have occurred. Reviewing access logs falls into the category of a detective control; these controls are covered in other GSA IT Security Procedural guides.

Best Practices for Authorization

Identification, authentication, and authorization must apply to the following:

- Personnel (whether GSA employees or contractors);
- Interconnections of systems and automated processes;
- Interconnections of devices.

Throughout the following best practices descriptions when the description addresses an AC control it is listed in parentheses.

Personnel Authorization Best Practices

The general activities for authorizing personnel to access IT resources are:

- Categorize positions, roles, and responsibilities for GSA employees and contractors.
- Screen personnel utilizing the GSA background investigation process.
- Obtain authorization for requested access rights. Determine whether to grant access rights and which access rights should be granted based on the job function of the requestor, privacy concerns and a signed authorization request.
- Provide the GSA and any system specific Rules of Behavior. Receive the required acknowledgement(s) from the requestor.
- Manage access rights by establishing authorized access, documenting, monitoring, and removing access rights in a timely manner, including periodically recertifying the need for the approved access.
- Document the processes.
- Retain documentation according to GSA documentation retention policies.

The following sections explain details for these activities and include references to NIST SP 800-53, Revision 5 AC controls. Other NIST control families impact access control decisions (e.g., Identification and Authentication, Personnel, and Physical and Environment) however this guide focuses on the AC controls while other GSA IT Security procedural guides and policies focus on the other NIST SP 800-53, Revision 5 control families. The NIST controls are listed by family code and number (e.g., AC-05).

Categorize Roles, Positions and Responsibilities

The GSA Office of Human Resources Management (OHRM) is responsible for assigning risk to all positions and establishing screening criteria for GSA employees, effectively categorizing all positions.

Docusign Envelope ID: 1636BF85-DA76-4F0E-964C-4C3DA19ABB87

For third-party personnel such as contractors, GSA system program managers and contracting officers must establish security requirements, including roles and responsibilities.

Separation of duties is an important consideration when defining roles and responsibilities (AC-05). Using the roles and responsibilities as a foundation, Data Owners can identify specific types of users that can be authorized to obtain access to each IT resource for functions such as:

- General user activities (e.g., resource or file access)
- System development (e.g., programs and databases)
- Technical operations and system or network administrators (e.g., accounts, permissions)
- Privacy accountability, audit and risk management (e.g., logs, alerts)

This process can be simplified by creating standard profiles describing access needs for each group and identifying the authorization process, nature and the extent of the access to each IT resource available for each function.

In special cases, the Data Owners may also identify any activities with an IT resource that do not require identification, authentication and authorization (AC-14). An example would be a website for the public providing general information. However, “anonymous” accounts should not be permitted.

Screen Personnel Utilizing Background Investigations

A background investigation of any potential personnel is required as part of the authorization process. Personnel are required to comply with GSA’s background investigating policies. For GSA employees, the Office of Mission Assurance Personnel Security Officer is responsible for the personnel screening process, while the CO/COR is responsible for contractor background investigations. The ISSO assists the AO, data owner, and CO/COR in ensuring that users have the required background investigations.

The investigation process verifies a person’s claimed identity and based on the level of investigation; the level of access permitted.

Grant Access Rights

When a person applies to become a user of one or more systems, that person’s supervisor must coordinate and arrange system access requests and verify the individual’s need-to-know (AC-02).

The applicable data owner must review and provide written authorization to access GSA resources (AC-02), based on need to know and least privilege (AC-06). The default access to any resource is DENY, but the data owner may grant other permissions based on the applicant’s job assignment.

An important consideration in granting access is to ensure separation of duties and this is the responsibility of the System Owner. Separation of duties (AC-05) helps to prevent a single user from having enough authorizations to inflict potential damage such as performing fraudulent actions. For example, a security administrator responsible for access controls should not be granted access to audit logs.

Docusign Envelope ID: 1636BF85-DA76-4F0E-964C-4C3DA19ABB87

Following direction from Data Owners, the ISSO in coordination with the system/network administrators are then responsible for establishing accounts. The account identifier for each user must be unique; in other words, shared accounts are not allowed (AC-02).

Figure E-1, Access Credentials, depicts how access is granted based on a verified identity and the System Owner and the data owner determining the type of access to the system (credentials) and to the data (authorizations).

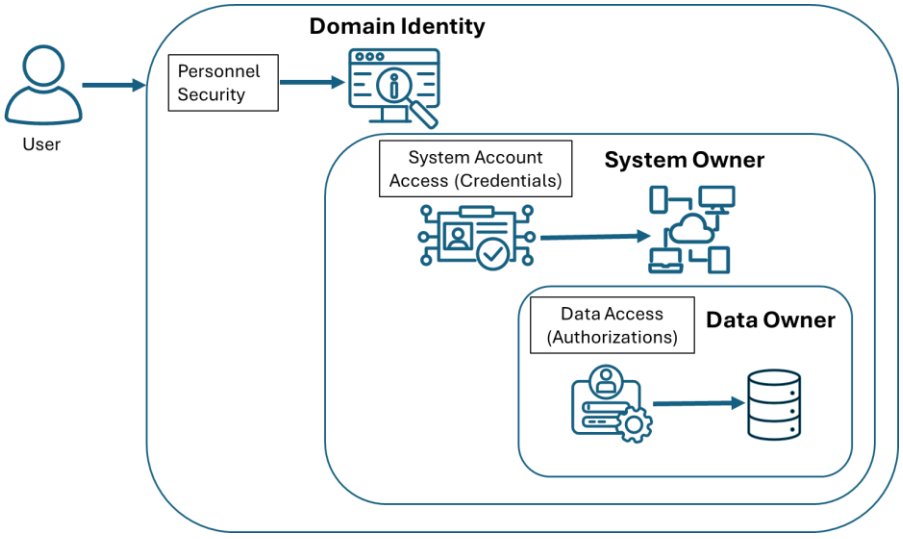

Figure E-1: Access Credentials

Authorization rights will allow the user to access designated data (e.g., a separated employee database) in designated ways (e.g., read, write, execute). Limits on writing (inputting) information may need to be particularly restricted. The combination of the authentication credentials and the authorization rights are applied by access control technologies and techniques to deny or allow requests for access to the data; these are discussed in a later chapter.

Special Case: In addition to authorizing access to internal systems, the AO must authorize access for individuals representing GSA to or from external information systems that are not under the control of GSA (AC-20). Examples include other federal or governmental (e.g., state, or tribal) information systems; non-governmental information systems; public access devices (e.g., through Internet cafes); and privately owned devices (e.g., home computers, personal digital assistants).

Manage Access Rights

Following the direction provided by System Owners, Data Owners and authorizing officials, the ISSO, and system/network administrators establish, maintain, and remove access rights to the system in accordance with GSA policy. See Figure E-2: Account Creation and Termination.

Accounts and authorization rights must be reviewed for change or revoked if an individual transfers, terminates, or changes the relationship with GSA under other circumstances (AC-02). Supervisors must arrange system access termination for all departing or resigning personnel on a timely basis.

Docusign Envelope ID: 1636BF85-DA76-4F0E-964C-4C3DA19ABB87

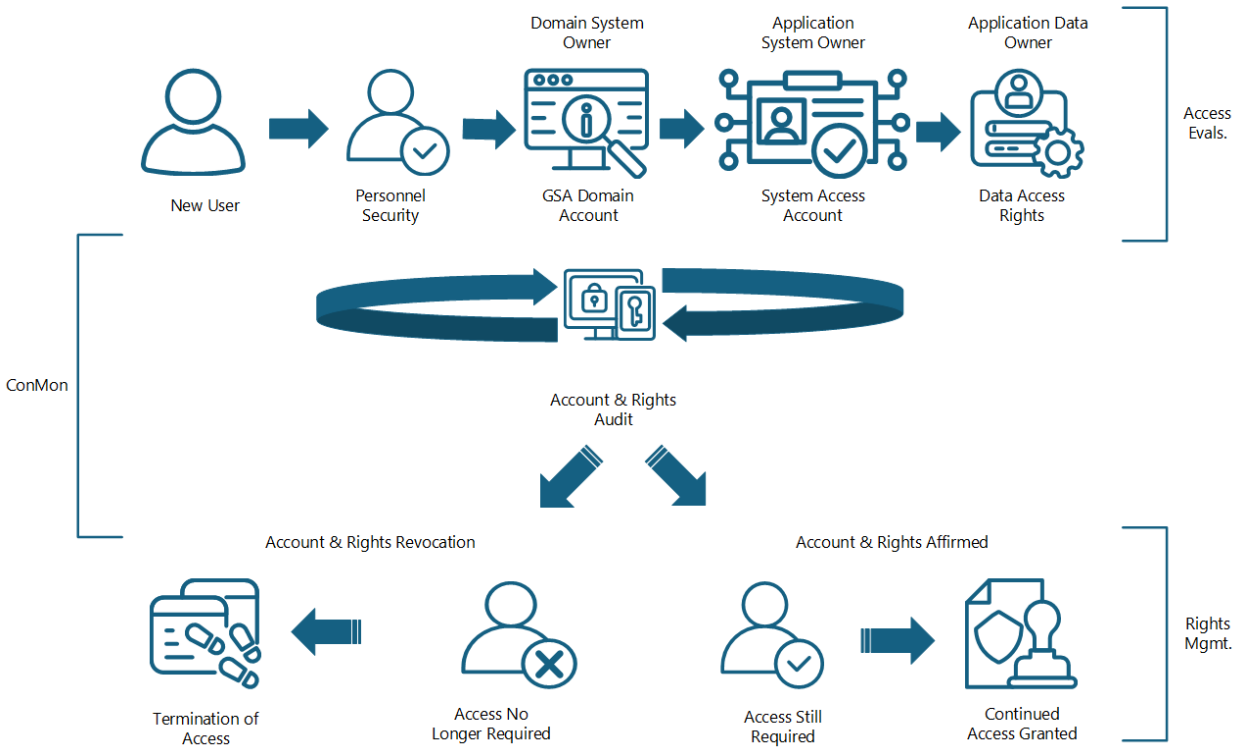

Figure E-2: Account Creation and Termination

The System Owner and the ISSO are also responsible for documenting all accounts for each resource, and the documentation must include confirmation that the user has read, understood, and agreed to abide by the policies of GSA, including all system Rules of Behavior.

In addition, System Owners, Data Owners, and ISSOs must manage Non-person entity (NPE) accounts for all systems, including establishing, activating, modifying, reviewing, disabling, and removing accounts. NPE accounts must be reviewed and validated the same as user accounts consistent with the SSPP to ensure its continued need for system access.

System owners and Data Owners are responsible for the accuracy and currency of the account credentials and authorizations for each user who is granted access. The documentation should clearly indicate what rights have been granted, when the accounts and the authorizations were last reviewed, and who granted and reviewed them. System owners and Data Owners must review and validate accounts and authorizations to ensure continued need for access.

Document the Processes

There must be a documented process for creating accounts and granting authorizations as well as for revocation of accounts and authorization. There must also be documented processes for periodic review and annual audit of access rights to ensure that each individual's access continues to meet GSA policy.

Best Practices for Technical Access Controls

Technical controls include the devices and software that enforce, monitor and control access. These controls limit access to data and data processing and communications systems.

Docusign Envelope ID: 1636BF85-DA76-4F0E-964C-4C3DA19ABB87

All GSA information systems must be configured to automatically manage the identification and authentication of users, automated processes, and devices, thereby controlling access and enforcing assigned authorizations (AC-03). ISSOs are responsible for administering the user identification and authentication scheme used in the system. Authenticators must follow GSA policies and procedural guides.

In addition to requiring identification and authentication at the system level, access control can be enforced at the application level, providing detailed restrictions on users.

The assigned authorizations must follow the concept of “least privilege” to limit users to only those resources and activities necessary to perform assigned job functions (AC-06). The access authorizations must also enforce separation of duties (AC-05).

Special Cases: Privileged rights such as “administrator” shall be restricted to authorized individuals as approved by the AO or ISSM.

The ability to input information must be limited to authorized personnel (AC-02, AC-03, AC-05, AC-06).

PII shall be made available only to those individuals with a business need to know.

Certain information on publicly available websites may not require identification and authentication by users; an example of such a website is www.gsa.gov. The appropriate individual(s) must decide whether specific data should be on the public website (AC-14, AC-22).

GSA information systems must employ the following automated controls:

1. Display the authorized GSA system use notification message (AC-08) before granting system access. The user must take explicit action to acknowledge the message before logging in. Messages other than the GSA message must be approved by the AO. The GSA CISO must be notified;
2. Identify and authenticate any user, process, or device before connecting to the information system;
3. Enforce a limit on consecutive unsuccessful access attempts (AC-07);
4. For High systems, limit the number of concurrent sessions for any user (AC-10);
5. For Moderate and High systems, lock a user session after a pre-determined time period of inactivity (AC-11);
6. For Moderate and High systems, terminate a remote session after a pre-determined time period of inactivity (AC-12, AC-17).
7. Disable accounts that are not used over a period of 90 days and require the user to request that access be restored (AC-02).

ISSOs and System/Network Administrators must employ mechanisms to control and monitor the following:

1. Remote access, such as over the public Internet or via a Virtual Private Network (VPN) connection (AC-17);
2. Wireless access (AC-18);
3. Access by portable and mobile devices such as laptops, tablets, or mobile phones (AC-19);
4. Access via an external information system (AC-20).

Docusign Envelope ID: 1636BF85-DA76-4F0E-964C-4C3DA19ABB87

5. Differences in access via atypical usage (AC-02(12))

All GSA information systems should enforce approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy. 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 (AC-04)

System Interconnection Authorization Best Practices

If a system is to be interconnected with another system outside the authorization boundary there must be an ISA/MOA in accordance with CIO-IT Security-24-125. The interconnection must be periodically reviewed, and such review must be documented.

In addition, any method of remote access (AC-17) to the information system must be approved by the System Owner under written authorization from the AO.

Device Authorization Best Practices

The GSA has established usage restrictions and implementation guidance in CIO-IT Security-12-67 for:

- Wireless devices (AC-18); and
- Portable and mobile devices (tablets, mobile phones, etc.) (AC-19).

Except for normal web access (e.g., using a browser from a wireless device), systems must include in their SSPPs if wireless access is specifically designed for accessing system components. Any wireless access to a system must be authorized as part of the system's ATO. This also applies to sharing of sensitive data or information, to include PII (AC-21).

Note: As stated in CIO-IT Security-12-67, "mobile devices are portable computing devices (i.e., smartphones, tablets). Laptops are specifically excluded from the scope of the guide since the security controls available for laptops are quite different from those available for smartphones and tablets. Mobile devices with minimal computing capability, such as basic cell phones, are also out of scope because of the limited security options available and the limited threats they face."

Media Protection Best Practices

Only authorized individuals may have access to storage media, including drives, tapes, CD-ROMs, DVDs, Thumb drives or disks (AC-20(02)). Storage media must be physically controlled and securely stored and encrypted if transported outside of controlled areas. See CIO-IT Security-06-32: Media Protection for additional guidance on media protection and CIO-IT Security-12-64 on physical protection.

Docusign Envelope ID: 1636BF85-DA76-4F0E-964C-4C3DA19ABB87

Appendix F: Definitions

All terms are consistent with the definitions from NIST's Glossary webpage. Definitions marked with an * are defined as listed for the purposes of this guide (i.e., not from the NIST webpage).

Access
Ability to make use of any information system (IS) resource.

Access Control
The process of granting or denying specific requests to: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities (e.g., federal buildings, military establishments and/or border crossing entrances).

Access Control List (ACL)
1. A list of entities, together with their access rights, that are authorized to have access to a resource.
2. A mechanism that implements access control for a system resource by enumerating the identities of the system entities that are permitted to access the resources.

Access Profile
Association of a user with a list of protected objects the user may access.

Account*
Is an identifier associated with a user that associates that identity with the data it is authorized to access, change and /or delete.

Accountability
The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.

Anonymous User*
A user that is not authenticated. Systems that sometimes grant access rights to Anonymous Users must do so with very few privileges. The access must be audited.

Authentication
Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

Authorization
Access privileges granted to a user, program, or process or the act of granting those privileges.

Availability
Ensuring timely and reliable access to and use of information.

Confidentiality
Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Credential
An object or data structure that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a Subscriber.

Identification
The process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system.

Docusign Envelope ID: 1636BF85-DA76-4F0E-964C-4C3DA19ABB87

Identity
A set of attributes that uniquely describe a person within a given context.

Integrity
Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

Least Privilege
The principle that a security architecture is designed so that each entity is granted the minimum system authorizations and resources that the entity needs to perform its function.

Privilege
A right granted to an individual, a program, or a process.

Subscriber
A party who has received a credential or authenticator from a Credential Service Provider.