## VERSION HISTORY/CHANGE RECORD

<table>
<thead>
<tr>
<th>Change Number</th>
<th>Person Posting Change</th>
<th>Change</th>
<th>Reason for Change</th>
<th>Page Number of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revision 2 – January 30, 2008</td>
<td>Scott / Heard</td>
<td>Changes made throughout the document to reflect FISMA, NIST and GSA CIO P 2100.1B requirements.</td>
<td>Updated to reflect and implement various FISMA, NIST and GSA CIO P 2100.1B requirements.</td>
<td>Various</td>
</tr>
<tr>
<td>2</td>
<td>Scott / Heard</td>
<td>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.</td>
<td>Updated to reflect the correlation of the CIO-IT Security Guides; and to further express policy within them as standalone documents</td>
<td>Various</td>
</tr>
<tr>
<td>3</td>
<td>Hummel / Windelberg</td>
<td>Changes throughout the document to correspond with update of the current version of GSA CIO P 2100</td>
<td>The most current version of GSA CIO P 2100 and more detailed guidance on implementing policy</td>
<td>Various</td>
</tr>
</tbody>
</table>

### Revision 3 – April 1, 2015

<table>
<thead>
<tr>
<th>Change Number</th>
<th>Person Posting Change</th>
<th>Change</th>
<th>Reason for Change</th>
<th>Page Number of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Sitcharing</td>
<td>Changes throughout to correspond with revisions made to CIO-IT-Security-06-30.</td>
<td>Updated to reflect correlation of the CIO-IT Security Guide and CIO P 2100.1.</td>
<td>Throughout</td>
</tr>
<tr>
<td>2</td>
<td>Heard</td>
<td>Changes the document to Implement ADM O 5440.667</td>
<td>Updated to reflect CISO GSA IT responsibilities</td>
<td>Throughout</td>
</tr>
<tr>
<td>3</td>
<td>Heard / Mott</td>
<td>Privacy access information included</td>
<td>Appendix J controls included in table 1 as well as explained within the guide</td>
<td>Throughout</td>
</tr>
</tbody>
</table>

### Revision 4 – May 8, 2017

<table>
<thead>
<tr>
<th>Change Number</th>
<th>Person Posting Change</th>
<th>Change</th>
<th>Reason for Change</th>
<th>Page Number of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Feliksa/Dean/ Klemens</td>
<td>Update to current format, style, and polices.</td>
<td>Updated to latest guide structure. Revised to reflect updates to Federal policies, NIST documents, and GSA processes.</td>
<td>Throughout</td>
</tr>
</tbody>
</table>
APPROVAL


5/8/2017

X Kurt Garbars
Kurt Garbars
GSA Chief Information Security Officer
Signed by: KURT GARBARS

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

1 Introduction .............................................................................................................................................. 1
  1.1 Purpose ............................................................................................................................................... 1
  1.2 Scope .................................................................................................................................................. 1
  1.3 Policy .................................................................................................................................................. 2
  1.4 References ......................................................................................................................................... 2

2 Roles and Responsibilities .................................................................................................................... 3
  2.1 The Chief Information Security Officer (CISO) ..................................................................................... 3
  2.2 Authorizing Official (AO) ..................................................................................................................... 3
  2.3 Information Systems Security Manager (ISSM) ................................................................................... 4
  2.4 Information System Security Officer (ISSO) ....................................................................................... 4
  2.5 System Owner ...................................................................................................................................... 4
  2.6 Data Owners ........................................................................................................................................ 5
  2.7 Contracting Officers (COs)/Contracting Officer Representatives (CORs) ........................................... 5
  2.8 Custodians .......................................................................................................................................... 6
  2.9 Authorized Users of IT Resources ......................................................................................................... 6
  2.10 GSA Personnel Security Officer/Office of Mission Assurance ........................................................... 6
  2.11 System/Network Administrators ........................................................................................................ 6
  2.12 Supervisors ....................................................................................................................................... 7

3 ACCESS CONTROL OVERVIEW ......................................................................................................... 7
  3.1 What are Access Controls? .................................................................................................................... 7
  3.2 Why Are Access Controls Important? ................................................................................................... 8

4 Access Controls Best Practices .......................................................................................................... 9
  4.1 Best Practices for Authorization ........................................................................................................... 9
    4.1.1 Personnel Authorization Best Practices .......................................................................................... 9
    4.1.2 System Interconnection Authorization Best Practices ................................................................. 13
    4.1.3 Device Authorization Best Practices ............................................................................................. 13
    4.1.4 Media Protection Best Practices ................................................................................................. 13
  4.2 Best Practices for Technical Access Controls ..................................................................................... 13

5 GSA Implementation Guidance for AC Controls ............................................................................... 15
  5.1 AC-1 Access Control Policy and Procedures ...................................................................................... 15
  5.2 AC-2 Account Management ................................................................................................................ 16
  5.3 AC-3 Access Enforcement .................................................................................................................... 18
  5.4 AC-4 Information Flow Enforcement ................................................................................................... 18
  5.5 AC-5 Separation of Duties .................................................................................................................... 18
  5.6 AC-6 Least Privilege ............................................................................................................................ 19
  5.7 AC-7 Unsuccessful Logon Attempts ..................................................................................................... 20
  5.8 AC-8 System Use Notification .............................................................................................................. 20
  5.9 AC-10 Concurrent Session Control ...................................................................................................... 21
  5.10 AC-11 Session Lock ............................................................................................................................ 21
  5.11 AC-12 Session Termination ................................................................................................................. 21
  5.12 AC-14 Permitted Actions without Identification or Authentication .................................................. 22
  5.13 AC-17 Remote Access ........................................................................................................................ 22

U.S. General Services Administration
5.14 AC-18 Wireless Access ........................................................................................................23
5.15 AC-19 Access Control for Mobile Devices ........................................................................23
5.16 AC-20 Use of External Information Systems ......................................................................24
5.17 AC-21 Information Sharing ................................................................................................25
5.18 AC-22 Publicly Accessible Content .................................................................................25

6 Summary ..................................................................................................................................26

Appendix A: Definitions ..............................................................................................................27

Appendix B: GSA CIO Order 2100.1 Policy Statements on Access Control .................................29
1 Introduction

Implementing an effective access control program and adhering to GSA CIO Order 2100.1, “GSA Information Technology (IT) Security Policy” and federal mandates are the best ways to ensure the protection of GSA systems and resources from loss, misuse, disclosure, or impairment. An effective program would carefully apply 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 4, “Security and Privacy Controls for Federal Information Systems and Organizations” in the Access Control (AC) family of security controls. Physical access controls are covered in GSA IT Security Procedural Guide CIO-IT Security-12-64, “Physical and Environmental Protection”. Personnel access controls are covered GSA’s Information Security Program Plan, and GSA’s personnel security policies.

Every GSA IT system must follow the access control practices identified in this guide. Any deviations from the security requirements established in GSA CIO Order 2100.1 must be coordinated by the Information Systems Security Officer (ISSO) through the appropriate Information Systems Security Manager (ISSM) and authorized by the Authorizing Official (AO). Any deviations, exceptions, waivers, or other conditions not following GSA policies and standards also must be forwarded to Office of the Chief Information Security Officer (OCISO) Policy and Compliance Division (ISP) at ispcompliance@gsa.gov to establish a record of the evidence regarding the item and any resultant Plan of Action and Milestones (POA&M).

The mechanisms associated with access control, when effectively applied, ensure that individuals or devices accessing or connecting to GSA’s IT resources are given access only to data and resources they authorized access based on their need-to-know and privileges needed to perform their job.

1.1 Purpose

The purpose of the guide is to provide guidance to implement GSA’s AC requirements as they apply to the NIST SP 800-53 AC control family and GSA CIO Order 2100.1. This guide provides GSA Federal employees and contractors with significant security responsibilities guidance and information for implementing access control features and functions for systems under their purview.

1.2 Scope

The procedures in this guide cover all GSA information and information systems to include those used, managed, or operated by a GSA employees or contractors on behalf of GSA. These procedures apply to all GSA employees and contractors.
1.3 Policy

The current version of GSA CIO Order 2100.1 has numerous policy statements pertaining to access controls. Some of the more important responsibilities and policies are summarized here; the parenthetical information indicates the chapter and paragraph of the pertinent policy statement. For a listing of access control responsibilities see Section 2, for policy details from the current version of GSA CIO Order 2100.1, see Appendix B.

- System owners must grant system access based on a valid need-to-know/need-to-share. (Chapter 2, 13.dd)
- System and data owners must ensure system access is restricted to authorized users. (Chapter 2, 13.ee, 14.c)
- System and data owners must ensure access authorization is appropriate at least annually. (Chapter 2, 13.m, 14.d)
- Information systems must operate in such a way that they run with the least amount of system privilege needed to perform a specific function and that system access is granted on a need to know basis. (Chapter 4, 2.u)
- All GSA systems must implement logical access controls to authorize or restrict the activities of users and system personnel to authorized transactions and functions. (Chapter 5, 2.b)
- Supervisors of GSA employees and CORs of GSA contractors must be responsible for coordinating and arranging system access requests for all new or transferring employees and for verifying an individual's need-to-know (authorization). (Chapter 4, 2.a(3))
- User authorizations must be verified annually for all information systems. (Chapter 4, 2.a(5))
- Users must utilize access rights based on a need to know. (Chapter 2, 17.i)
- Written management authorization for system interconnection, based upon the acceptance of risk to the IT system, must be obtained from the Authorizing Officials of both systems prior to connecting a system not under a single Authorizing Official's control in accordance with NIST SP 800-47, “Security Guide for Interconnecting Information Technology Systems”. Per NIST 800-47, an interconnection is the direct connection of two or more IT systems for the purpose of sharing data and other information resources through a pipe, such as ISDN, T1, T3, DS3, VPN, etc. (Chapter 3, 2.i(1))

1.4 References

- GSA CIO Order 2100.1, “GSA Information Technology (IT) Security Policy”
- GSA CIO Order 2104.1, “GSA Information Technology (IT) General Rules of Behavior”
- CIO-IT Security-12-64, “Physical and Environmental Protection”
- GSA Information Security Program Plan
Roles and Responsibilities

There are many roles associated with implementing an effective access control program. System owners for each information system are responsible for ensuring that access control processes exist for their specific system and that the appropriate people have been assigned access control related roles and responsibilities.

The System Program Managers/Project Managers have direct responsibility to ensure effective implementation and management of GSA’s access controls requirements for each of their systems. The roles and responsibilities provided in this section have been extracted or paraphrased from GSA CIO Order 2100.1 or summarized from GSA and Federal guidance. Throughout this guide requirements for implementing access control are described. Complete roles and responsibilities for agency management officials and roles with significant IT Security responsibilities are defined in GSA CIO Order 2100.1.

2.1 The Chief Information Security Officer (CISO)

Responsibilities include the following:

- Reporting to the GSA CIO on the implementation and maintenance of the GSA’s IT Security Program and Security Policies;
- Implementing and overseeing GSA’s IT Security Program by developing and publishing IT Security Procedural Guides that are consistent with this policy;
- Directing the planning and implementation of the GSA IT Security Awareness and Privacy Training Program to ensure agency personnel, including contractors, receive appropriate security and privacy awareness training based on their roles and access to information and information systems;
- Periodically assessing risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency.

2.2 Authorizing Official (AO)

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 policy 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;

• Ensuring a plan of action and milestones (POA&M) item is established and managed to address AC Controls that are not fully implemented.

2.3 Information Systems Security Manager (ISSM)

Responsibilities include the following:

• Ensuring adherence and proper implementation of GSA’s IT Security Policy;
• Ensuring assessment and authorization support documentation is developed and maintained (including the implementation of access controls);
• Managing POA&Ms regarding AC controls for all systems under their purview;
• Ensuring ISSOs and System Owners are maintaining POA&Ms regarding AC controls for their systems, including taking remediation actions according to scheduled milestones.

2.4 Information System Security Officer (ISSO)

Responsibilities include the following:

• Ensuring the system is operated, used, maintained, and disposed of in accordance with internal security policies and procedures. Necessary security controls (including access controls) should be in place and operating as intended;
• Assisting the Authorizing Official, Data Owner and Contracting Officer / Contracting Officer Representative in ensuring users have the required background investigations, the required authorization and need-to-know, and are familiar with internal security practices before access is granted to the system;
• Reviewing system role assignments to validate compliance with principles of least privilege;
• Assisting in the identification, implementation, and assessment of a system’s security controls, including common controls.
• Developing POA&Ms regarding AC controls for all systems under their purview

2.5 System Owner

Responsibilities include the following:

• Ensuring their systems and the data each system processes have necessary security controls in place (including access controls) and are operating as intended and protected in accordance with GSA regulations and any additional guidelines established by the ISSO or ISSM;
• Conducting annual reviews and validations of system users’ accounts to ensure the continued need for access to a system and verify users’ authorizations (rights/privileges);
• Defining, implementing, and enforcing detailed separation of duties by ensuring that 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 IS SO 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 (including the AC control family) for their respective systems IAW IT Security Procedural Guide: Plan of Action and Milestones (POA&M), CIO-IT Security-09-44;

Ensuring proper separation of duties for GSA IT system maintenance, management, and development processes;

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;

Working with Data Owners with assistance from the ISSO, will ensure system access is restricted to authorized users that have completed required background investigations, are familiar with internal security practices, and have completed requisite security and privacy awareness training programs, such as the annual IT Security & Privacy Act training curriculum.

2.6 Data Owners

Responsibilities include the following:

- Working with the system owner, with assistance from the ISSO, to ensure system access is restricted to authorized users that have completed required background investigations, are familiar with internal security practices, and have completed requisite security and privacy awareness training programs;
- Ensuring system access authorizations enforce job function alignment, separation of duties, and are based on the principle of need-to-know/need-to-share that is determined during the account authorization process and the intended system usage.
- Reviewing access authorization listings and determining whether they remain appropriate at least annually;
- Coordinating with IT security personnel including the ISSM and IS SO and system owners to ensure implementation of system and data security requirements.

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

Responsibilities include the following:

- Working with the CISO to facilitate the monitoring of contract performance for compliance with the agency’s information security policy;
- Identifying and initiating contractor background investigations in collaboration with the GSA Personnel Security Officer;
- Ensuring that all IT acquisitions include the appropriate security requirements in each contract and task order;
- Ensuring that the appropriate security and privacy contracting language is incorporated in each contract and task order;
2.8 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.

2.9 Authorized Users of IT Resources

Responsibilities include the following:

- Complying with all GSA security policies and procedures.
- Complying with security training, education, and awareness sessions commensurate with their duties.
- 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 before leaving their workstation;
- Utilizing assigned privileged access rights (power user, database administrator, web site administrator, etc.) to a computer based on need to know.

2.10 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.

2.11 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 know;
- Ensuring system/network administrators 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.

- Creating, modifying, and deleting accounts, access rights/privileges, and roles in cooperation with the system owner, data owner, and ISSM/ISSO.

## 2.12 Supervisors

Responsibilities of the Supervisors 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 for verifying an individual’s need-to-know (authorization);
- Coordinating and arranging system access termination for all departing or resigning 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.

## 3 ACCESS CONTROL OVERVIEW

### 3.1 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 system interconnection.

Identification, authentication, and authorization are key terms regarding access control. Each user of a resource should have a unique identifier. 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 Authorizing Official of the resource. Authentication involves attempting to verify the user’s identity through one or more credentials; e.g., an ID card, a password, a signature, or a biometric such as a fingerprint. Authorization determines what the individual 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 assigned
to the roles; in role-based access controls, users obtain only the rights assigned to the group (role) as a whole.

### 3.2 Why Are Access Controls 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 agency 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, least privilege access);
- Limiting access to sensitive resources (e.g., financial records, security software programs, or data centers);
- Ensuring the agency complies with Federal regulations and mandates to reduce or eliminate federal reprimands.

Without effective access controls, GSA increases the possibility of information loss or theft, regardless of its sensitivity, and limits the control of who has access to that 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 action of users of an IT resource, whether it is a system or its data.

The following section explains best practices for access controls, addressing:

- Authorizations, whether for personnel, system interconnections, or devices
- Technical access controls for information systems.
4 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.

4.1 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.

4.1.1 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 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 control families. The NIST controls are listed by family cod and number (e.g., AC-5).
4.1.1.1 **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.

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-5). 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.

4.1.1.2 **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 Authorizing Official (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.

4.1.1.3 **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-2).
The applicable Data Owner must review and provide written authorization to access GSA resources (AC-2), based on need to know and least privilege (AC-6). 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-5) 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.

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-2).

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

**Figure 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, etc.). 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 Authorizing Official 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 or personal digital assistants).
4.1.1.4 Manage Access Rights

Following the direction by System Owners, Data Owners and Authorizing Officials, the ISSO, System/Network Administrators establish, maintain and remove access rights to the system in accordance with GSA policy. See Figure 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-2). Supervisors must arrange system access termination for all departing or resigning personnel on a timely basis.

![Figure 2: Account Creation and Termination](image)

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.

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.

4.1.1.5 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.
4.1.2 System Interconnection Authorization Best Practices

If a system is to be interconnected with another system outside the accreditation boundary and under a different Authorizing Official, the System Owner must obtain written authorization to do so from both Authorizing Officials. There must also be a written Interconnection Security Agreement. 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 Authorizing Official.

4.1.3 Device Authorization Best Practices

GSA has established usage restrictions and implementation guidance for:

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

The System Owner must obtain written authorization from the Authorizing Official to permit any such devices to connect to the information system. This also applies to sharing of sensitive data or information, to include Personally Identifiable Information (AC-21).

4.1.4 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 (2)). Storage media must be physically controlled and securely stored and encrypted if transported outside of controlled areas.

4.2 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.

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-3). 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-6). The access authorizations must also enforce separation of duties (AC-5).
**Special Cases:** Privileged rights such as “administrator” shall be restricted to authorized individuals as approved by the Authorizing Official or ISSM.

The ability to input information must be limited to authorized personnel (AC-2, AC-3, AC-5, AC-6).

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 or not specific data should be on the public website (AC-14).

GSA information systems must employ the following automated controls:

1. Display the authorized GSA system use notification message (AC-8) 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-7);
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-2).

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).
5. Differences in access via atypical usage (AC-2 (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-4).

5 **GSA Implementation Guidance for AC Controls**

The GSA-defined parameter settings included in the control requirements are offset by brackets in the control text. As stated in Section 1.2, Scope, the requirements in this guide apply to GSA Federal employees and contractors who are involved in access control of GSA information systems and data. Most of the GSA implementation guidance sections for AC controls refer to Section 4 and Appendix B where best practices and requirements for implementing AC controls is contained. Any additional instructions/requirements for contractor systems will be included in the additional contractor system considerations portion of each control section. The term “None” for contractors means that there are no additional implementation instructions for contractors, they still must adhere to GSA guidance, policies, and procedures.

AC-1, Access Control Policy and Procedures, has been identified as a Common Control for all GSA/Internally operated systems by GSA and as a Hybrid Control for contractor systems. The rest of the AC controls, when included in a system’s control set, either are provided as a Common Control by a major information system, a system specific control by the system, or as a Hybrid Control with shared responsibilities for control implementation.

5.1 **AC-1 Access Control Policy and Procedures**

**Control:** The organization:

- Develops, documents, and disseminates to [Information System Security Manager, Information System Security Officer, System Owners (e.g., System Program Managers, System Project Managers), Acquisitions/Contracting Officers, Custodians]:
  1. An access control policy that addresses purpose, scope, responsibilities, management commitment, coordination among organizational entities, and compliance; and
  2. Procedures to facilitate the implementation of the access control policy and associated access controls; and
- Reviews and updates the current:
  1. Access control policy [biennially]; and
  2. Access control procedures [biennially].

**GSA Implementation Guidance:** Control AC-1 is applicable at all FIPS 199 levels.

Access Control policy and procedures is a common control provided by the GSA OCISO Policy and Compliance Division (ISP). Access Control Policy is included in CIO 2100.1, "GSA IT Security Policy” Chapter 5, Policy on Technical Controls. The policy states, "All GSA systems must implement logical access controls to authorize or restrict the activities of users and system personnel to authorized transactions and functions." GSA OCISO ISP has also defined agency-wide access control procedures in GSA IT Security Procedural Guide CIO-IT Security-01-07,
“Access Control” (this guide). GSA’s security policy and procedural guides are disseminated via the IT Security webpage.

CIO 2100.1 and GSA CIO-IT Security-01-07 are reviewed/updated biennially.

Additional Contractor System Considerations:
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).

5.2 AC-2 Account Management

Control: The organization:

a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: [minimum - System Administrator, Network Administrator, Application Administrator, Database Administrator, GSA S/SO or Contractor recommendation to be approved and accepted by the GSA AO];
b. Assigns account managers for information system accounts;
c. Establishes conditions for group and role membership;
d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
e. Requires approvals by [System Owner and GSA Authorizing Official] for requests to create information system accounts;
f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [GSA CIO-IT Security-01-01, Identification and Authentication, GSA CIO-IT Security-01-07, Access Control, and GSA-defined procedures or conditions (as applicable)];
g. Monitors the use of information system accounts;
h. Notifies account managers:
   a. When accounts are no longer required;
   b. When users are terminated or transferred; and
   c. When individual information system usage or need-to-know changes;
i. Authorizes access to the information system based on:
   a. A valid access authorization;
   b. Intended system usage; and
   c. Other attributes as required by the organization or associated missions/business functions;
j. Reviews accounts for compliance with account management requirements [annually]; and
k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

Control Enhancements:
(1) Account Management | Automated System Account Management. The organization employs automated mechanisms to support the management of information system accounts;
(2) Account Management | Removal of Temporary / Emergency Accounts. The information system automatically [disables] temporary and emergency accounts after [no more than 90 days];
(3) Account Management | Disable Inactive Accounts. The information system automatically disables inactive accounts after [90 Days for User Level Accounts, GSA S/SO or Contractor recommended time period to be approved and accepted by the GSA AO for non-user level accounts];
(4) Account Management | Automated Audit Actions. The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [Administrators (Application, System, Network, etc.), Information System Security Officer, Information System Security Manager, System Program Managers, and System Project Managers];
(5) Account Management | Inactivity Logout. The organization requires that users log out when [completing their workday];
(11) Account Management | Usage Conditions. The information system enforces [GSA S/SO or Contractor recommended circumstances and/or usage conditions to be approved and accepted by the GSA AO] for [GSA S/SO or Contractor recommended information system accounts to be approved and accepted by the GSA AO];
(12) Account Management | Account Monitoring/Atypical Usage.
   a. Monitors information 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. Reports atypical usage of information system accounts to [Information System Security Officer and the GSA OCISO].
(13) Account Management | Disable Accounts for High-Risk Individuals. The organization disables accounts of users posing a significant risk within [GSA S/SO or Contractor recommended time period to be approved and accepted by the GSA AO] of discovery of the risk.

**GSA Implementation Guidance:** Control AC-2 is applicable at all FIPS 199 levels. Enhancement AC-2 (1), (2), (3), and (4) are applicable at FIPS 199 Moderate and High levels. Enhancement AC-2 (5), (11), (12), and (13) is also applicable at the FIPS 199 High level.

Section 4 and Appendix B of this guide, GSA CIO-IT Security-01-01, and CIO 2100.1 describe best practices, procedures, and requirements for implementing AC-2 and its enhancements for GSA systems.

**Additional Contractor System Considerations:** None.
5.3 AC-3 Access Enforcement

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

**GSA Implementation Guidance:** Control AC-3 is applicable at all FIPS 199 levels.

Section 4 and Appendix B of this guide, GSA CIO-IT Security-01-01, and CIO 2100.1 describe best practices, procedures, and requirements for implementing AC-3 for GSA systems.

**Additional Contractor System Considerations:** None.

5.4 AC-4 Information Flow Enforcement

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

**GSA Implementation Guidance:** Control AC-4 is applicable at FIPS 199 Moderate and High levels.

Section 4 and Appendix B of this guide, GSA CIO-IT Security-01-01, and CIO 2100.1 describe best practices, procedures, and requirements for implementing AC-4 for GSA systems.

**Additional Contractor System Considerations:** None.

5.5 AC-5 Separation of Duties

**Control:** The organization:

a. Separates [GSA S/SO or Contractor recommended duties of individuals, based on roles and responsibilities, to be approved and accepted by the GSA AO ];

b. Documents separation of duties of individuals; and

c. Defines information system access authorizations to support separation of duties.

**GSA Implementation Guidance:** Control AC-5 is applicable at FIPS 199 Moderate and High levels.

Section 4 and Appendix B of this guide, GSA CIO-IT Security-01-01, and CIO 2100.1 describe best practices, procedures, and requirements for implementing AC-5 for GSA systems.

**Additional Contractor System Considerations:** None.
5.6  AC-6 Least Privilege

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

**Control Enhancements:**

1. **Least Privilege | Authorize Access to Security Functions.** The organization explicitly authorizes access to [GSA S/SO or Contractor recommended security functions (deployed in hardware, software, and firmware) and security-relevant information to be approved and accepted by the GSA AO];

2. **Least Privilege | Non-Privileged Access For Non-Security Functions.** The organization requires that users of information 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;

3. **Least Privilege | Network Access to Privileged Commands.** The organization authorizes network access to [all privileged commands (i.e., any command requiring privileges above a standard user)] only for [GSA S/SO or Contractor recommended compelling operational needs as approved by the AO] and documents the rationale for such access in the security plan for the information system;

4. **Least Privilege | Privileged Accounts.** The organization restricts privileged accounts on the information system to [GSA S/SO or Contractor recommended employees and contractors as approved by the AO];

5. **Least Privilege | Auditing Use of Privileged Functions.** The information system audits the execution of privileged functions;

6. **Least Privilege | Prohibit Non-Privileged Users From Executing Privileged Functions.** The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

**GSA Implementation Guidance:** Control AC-6, AC-6 (1), (2), (5), (9), and (10) are applicable at FIPS 199 Moderate and High levels. Enhancement AC-6 (3) is also applicable at the FIPS 199 High level.

Section 4 and Appendix B of this guide, GSA CIO-IT Security-01-01, and CIO 2100.1 describe best practices, procedures, and requirements for implementing AC-6 and its enhancements for GSA systems.

**Additional Contractor System Considerations:** None.
5.7 AC-7 Unsuccessful Logon Attempts

Control: The organization:

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

GSA Implementation Guidance: Control AC-7 is applicable at all FIPS 199 levels.

Section 4 and Appendix B of this guide, GSA CIO-IT Security-01-01, and CIO 2100.1 describe best practices, procedures, and requirements for implementing AC-7 for GSA systems.

Additional Contractor System Considerations: None.

5.8 AC-8 System Use Notification

Control: The information system:

  a. Displays to users \([\text{a system use notification message or banner as defined in GSA CIO Order 2100.1}]\) before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that:
      1. Users are accessing a U.S. Government information system;
      2. Information system usage may be monitored, recorded, and subject to audit;
      3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and
      4. Use of the information system indicates consent to monitoring and recording;
  b. Retains 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 information system; and
  c. For publicly accessible systems:
      1. Displays system use information \([\text{when accessed via logon interfaces with human users}]\), before granting further access;
      2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
      3. Includes a description of the authorized uses of the system.

GSA Implementation Guidance: Control AC-8 is applicable at all FIPS 199 levels.

Section 4 and Appendix B of this guide, GSA CIO-IT Security-01-01, and CIO 2100.1 describe best practices, procedures, and requirements for implementing AC-8 for GSA systems.

Additional Contractor System Considerations: None.
5.9 AC-10 Concurrent Session Control

**Control:** The information system limits the number of concurrent sessions for each [user] to [GSA S/50 or Contractor recommended number to be approved and accepted by the GSA AO].

**GSA Implementation Guidance:** Control AC-10 is applicable at the FIPS 199 High level.

Section 4 and Appendix B of this guide, GSA CIO-IT Security-01-01, and CIO 2100.1 describe best practices, procedures, and requirements for implementing AC-10 for GSA systems.

**Additional Contractor System Considerations:** None.

5.10 AC-11 Session Lock

**Control:** The information system:

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

**Control Enhancements:**

(1) Session Lock | Pattern-Hiding Displays. The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.

**GSA Implementation Guidance:** Control AC-11 and AC-11 (1) are applicable at FIPS 199 Moderate and High levels.

Section 4 and Appendix B of this guide, GSA CIO-IT Security-01-01, and CIO 2100.1 describe best practices, procedures, and requirements for implementing AC-11 for GSA systems.

**Additional Contractor System Considerations:** None.

5.11 AC-12 Session Termination

**Control:** The information system automatically terminates a user session after [(a) A remote access connection after thirty (30) minutes of inactivity; (b) An Internet accessible application session after thirty (30) minutes of inactivity; or (c) A non-interactive user session after thirty (30) – sixty (60) minutes of inactivity. Static web sites and long running operations (e.g., batch jobs) are not subject to this time limit].

**GSA Implementation Guidance:** Control AC-12 is applicable at the FIPS 199 Moderate and High levels.
Section 4 and Appendix B of this guide, GSA CIO-IT Security-01-01, and CIO 2100.1 describe best practices, procedures, and requirements for implementing AC-12 for GSA systems.

Additional Contractor System Considerations: None.

5.12 AC-14 Permitted Actions without Identification or Authentication

Control: The organization:

a. Identifies \[no user actions\] that can be performed on the information system without identification or authentication consistent with organizational missions/business functions; and
b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.

GSA Implementation Guidance: Control AC-14 is applicable at all FIPS 199 levels.

Section 4 and Appendix B of this guide, GSA CIO-IT Security-01-01, and CIO 2100.1 describe best practices, procedures, and requirements for implementing AC-14 for GSA systems.

Additional Contractor System Considerations: None.

5.13 AC-17 Remote Access

Control: The organization:

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

Control Enhancements:

1. Remote Access | Automated Monitoring / Control. The information system monitors and controls remote access methods;
2. Remote Access | Protection of Confidentiality / Integrity Using Encryption. The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions;
3. Remote Access | Managed Access Control Points. The information system routes all remote accesses through [GSA network access control points or network access control points per GSA S/SO or Contractor recommendation to be approved and accepted by the GSA AO] managed network access control points;
4. Remote Access | Privileged Commands / Access. The organization:
   a. Authorizes the execution of privileged commands and access to security-relevant information via remote access only for \[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. 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 security scans noted in CIO 2100.1, Chapter 5, Paragraph 2.v(2)); and 

b. Documents the rationale for such access in the security plan for the information system.

**GSA Implementation Guidance:** Control AC-17 is applicable at all FIPS 199 levels. AC-17 (1), (2), (3), and (4) are applicable at FIPS 199 Moderate and High levels.

Section 4 and Appendix B of this guide, GSA CIO-IT Security-01-01, and CIO 2100.1 describe best practices, procedures, and requirements for implementing AC-17 for GSA systems.

**Additional Contractor System Considerations:** None.

### 5.14 AC-18 Wireless Access

**Control:** The organization:

a. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and 

b. Authorizes wireless access to the information system prior to allowing such connections.

**Control Enhancements:**

1. **Wireless Access | Authentication and Encryption.** The information system protects wireless access to the system using authentication of [users and device] and encryption; 

4. **Wireless Access | Restrict Configurations by Users.** The organization identifies and explicitly authorizes users allowed to independently configure wireless networking capabilities; 

5. **Wireless Access | Antennas / Transmission Power Levels.** The organization selects radio antennas and calibrates transmission power levels to reduce the probability that usable signals can be received outside of organization-controlled boundaries.

**GSA Implementation Guidance:** Control AC-18 is applicable at all FIPS 199 levels. AC-18 (1) is applicable at the FIPS 199 Moderate and High levels. AC-18 (4) and (5) are also applicable at the FIPS 199 High level.

Section 4 and Appendix B of this guide, GSA CIO-IT Security-01-01, and CIO 2100.1 describe best practices, procedures, and requirements for implementing AC-18 and its enhancements for GSA systems.

**Additional Contractor System Considerations:** None.

### 5.15 AC-19 Access Control for Mobile Devices

**Control:** The organization:
a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and
b. Authorizes the connection of mobile devices to organizational information systems.

Control Enhancements:

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

GSA Implementation Guidance: Control AC-19 is applicable at all FIPS 199 levels. AC-19 (5) is applicable at FIPS 199 Moderate and High levels.

Section 4 and Appendix B of this guide, GSA CIO-IT Security-01-01, and CIO 2100.1 describe best practices, procedures, and requirements for implementing AC-19 and its enhancement for GSA systems.

Additional Contractor System Considerations: None.

5.16 AC-20 Use of External Information Systems

Control: The organization:

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

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

Control Enhancements:

(1) Use of External Information Systems | Limits on Authorized Use. The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization:
   a. Verifies the implementation of required security controls on the external system as specified in the organization’s information security policy and security plan; or
   b. Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.
(2) Use of External Information Systems | Portable Storage Devices. The organization [restricts] the use of organization-controlled portable storage devices by authorized individuals on external information systems.
GSA Implementation Guidance: Control AC-20, (1), and (2) are applicable at all FIPS 199 levels.

Section 4 and Appendix B of this guide, GSA CIO-IT Security-01-01, and CIO 2100.1 describe best practices, procedures, and requirements for implementing AC-20 and its enhancements for GSA systems.

Additional Contractor System Considerations: None.

5.17 AC-21 Information Sharing

Control: The organization:

a. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for [GSA S/So or Contractor recommended information sharing circumstances where user discretion is required to be approved and accepted by the GSA AO]; and
b. Employs [GSA S/So or Contractor recommended automated mechanisms or manual processes to be approved and accepted by the GSA AO] to assist users in making information sharing/collaboration decisions.

GSA Implementation Guidance: Control AC-21 is applicable at FIPS 199 Moderate and High levels.

Section 4 and Appendix B of this guide, GSA CIO-IT Security-01-01, and CIO 2100.1 describe best practices, procedures, and requirements for implementing AC-21 for GSA systems.

Additional Contractor System Considerations: None.

5.18 AC-22 Publicly Accessible Content

Control: The organization:

a. Designates individuals authorized to post information onto a publicly accessible information system;
b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;
c. Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and
d. Reviews the content on the publicly accessible information system for nonpublic information [quarterly] and removes such information, if discovered.

GSA Implementation Guidance: Control AC-22 is applicable at all FIPS 199 levels.

Section 4 and Appendix B of this guide, GSA CIO-IT Security-01-01, and CIO 2100.1 describe best practices, procedures, and requirements for implementing AC-22 for GSA systems. GSA CIO
Orders 9297.1 CIO GSA Data Release Policy and 2140.1 Management of GSA’s Total Web Presence provide additional information on the release of data and public content (web) data.

**Additional Contractor System Considerations:** None.

6 Summary

Access controls are required to ensure the confidentiality, integrity, availability, accountability and assurance of IT resources and facilities.

Effective access controls established and implemented for GSA IT resources assist the agency in accomplishing the stated mission, complying with federal mandates and the GSA IT Security Policy. Once effective controls have been established, they must be maintained through an ongoing effort and continuously monitored to ensure that the access controls remain effective in mitigating risks.

Where there is a conflict between NIST guidance and GSA guidance, contact the OCISO, ISP Division for guidance, at ispcompliance@gsa.gov.
Appendix A: Definitions

All terms are consistent with the definitions contained within the National Institute of Standards and Technology Interagency or Internal Report (NISTIR) 7298, Revision 2, Glossary of Key Information Security Terms. Definitions marked with an * are defined as listed for the purposes of this guide.

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 permissions associated with an object. The list specifies who or what is allowed to access the object and what operations are allowed to be performed on the object.

2. A mechanism that implements access control for a system resource by enumerating the system entities that are permitted to access the resource and stating, either implicitly or explicitly, the access modes granted to each entity.

Access Profile

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

Account *

Is an identifier associated with a profile that associates an authenticated 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.

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 security objective of granting users only those accesses they need to perform their official duties.

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

Subscriber
A party who receives a credential or token from a CSP (Credentials Service Provider) and becomes a claimant in an authentication protocol.
Appendix B: GSA CIO Order 2100.1 Policy Statements on Access Control

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

Chapter 3 of GSA CIO Order 2100.1 states:

a. Rules of the System (Chapter 3, Paragraph 2.h)

   (1) Authorized users must be provided written Rules of Behavior IAW GSA Order CIO 2104.1A before being allowed access into any GSA, non-public information system;

   (2) The user must acknowledge receipt of these rules through a positive action.

b. System interconnections/information sharing (Chapter 3, Paragraph 2.i)

   (1) Written management authorization for system interconnection, based upon the acceptance of risk to the IT system, must be obtained from the AOs of both systems prior to connecting a system not under a single AO’s control IAW NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems. Per NIST 800-47, an interconnection is the direct connection of two or more IT systems for the purpose of sharing data and other information resources through a pipe, such as ISDN, T1, T3, DS3, VPN, etc.

   (2) If GSA systems interconnect, they must connect using a secure methodology that provides security commensurate with the acceptable level of risk as defined in the system security plan and that limits access only to the information needed by the other system.

   (3) All interconnections between GSA and external entities including off-site contractors or Federal agency/departments must be approved by the AO and concurred by the GSA CISO, and reviewed on an annual basis, at a minimum.

c. Contractors and outsourced operations (Chapter 3, Paragraph 2.l) Implement appropriate safeguards to protect GSA information and information systems from unauthorized access throughout all phases of a contract. Review contracts to ensure that information security is appropriately addressed in the contracting language. GSA CIO-IT Security-09-48 establishes the security language for GSA IT acquisitions contracts involving contractors. All applicable NIST 800-53 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 Authorizing Official and the CISO. Any controls tailored out of the baseline must have the rationale for the decision documented in the system’s SSP.

Chapter 4 of GSA CIO Order 2100.1 states:
(3) Users must avoid the following prohibited e-mail and social media usages:
   (a) Transmitting unsolicited commercial announcements or advertising material, unless approved by management in advance.
   (b) Transmitting any material pertaining to GSA, the Federal Government, or any agency employee or official that is libelous or defamatory.
   (c) Transmitting sexually explicit or offensive material, non-business related large attachments, chain letters, un-authorized mass mailings, or intentionally sending a virus/worm.

(4) Personal use of Government IT systems for Internet access must be kept to a minimum and must not interfere with official system use or access.

(5) Users must avoid prohibited Internet usages including:
   (a) Unauthorized attempts to break into any computer, whether belonging to GSA or another organization.
   (b) Browsing sexually explicit, gambling sites or hate-based web sites.
   (c) Using Internet access for personal gain (i.e., making use of GSA resources for commercial purposes or in support of for profit activities such as running a private business).
   (d) Theft of copyrighted or otherwise legally protected material, including copying without permission.
   (e) Sending or posting sensitive material such as GSA building plans or financial information outside of the GSA network.
   (f) Automatically forwarding e-mail messages from GSA e-mail addresses to any non-Federal e-mail account(s) or address(es).
   (g) Sending e-mail messages including sensitive information, such as PII, as deemed by the Data Owner, without GSA provided encryption. Certified encryption modules must be used IAW FIPS PUB 140-2, Security requirements for Cryptographic Modules.

(6) If PII needs to be e-mailed outside the GSA network, encryption is required. Instructions can be found on the privacy web page in the section “Documents for Download.” Your e-mail will be blocked if Social Security Numbers are sent unencrypted.

(7) GSA prohibits an employee or contractor supporting GSA from creating or sending information using a non-official GSA electronic messaging account (i.e., company or personal email account).

(8) Additional guidance regarding GSA’s policy on email is available in GSA Orders CIO 2160.2 GSA Electronic Messaging and Related Services; ADM 7800.11, Personal Use of Agency Office Equipment; CIO 2104.1, GSA Information Technology (IT) General Rules of Behavior; and CIO P 2165.1, GSA Internal Telecommunications Management. Detailed guidance on social media is available in The Social Media Navigator, GSA’s Guide to the Use of Social Media, April 2011 or current.
b. **Separation of duties (FIPS 199 Moderate and High Impact Systems Only) (Chapter 4, Paragraph 2.1)**

(1) 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;

(2) 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;

(3) Every S/SO/R 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 increase the risk that unauthorized modifications to programs may be implemented into production systems, which could introduce vulnerabilities and negatively impact the integrity and availability of data generated and stored in the system;

(4) Document job descriptions and roles 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;

(5) Establish formal procedures to guide personnel in performing their duties, with identification of prohibited actions;

(6) Duties shall be segregated among users so that 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 that requires 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 that requires 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 that exceeds some limit requiring a supervisor’s review and approval);

(7) Ensure proper separation of duties for GSA IT system maintenance, management, and development processes;
(8) Information systems must enforce separation of duties through assigned access authorizations;

(9) Since critical processes can span separate and distinct applications and systems, each S/SO/R 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 that may span multiple IT systems or applications to uncover conflicts that may not be 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);

(10) Every S/SO/R must establish physical and logical access controls to enforce separation of duties policy and alignment with organizational and individual job responsibilities;

(11) Conduct annual assessments to review the effectiveness of control techniques, with an emphasis on activities that cannot 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);

(12) Review access authorization listings to determine whether they remain appropriate at least annually;

(13) Conduct annual reviews of staff training records to ensure annual Privacy Act, Security Training, and application specific training was completed for all users. The records shall be forwarded to application ISSO/System Owners as part of the annual recertification efforts.

c. Least Privilege (Chapter 4, Paragraph 2.u)

(1) Information systems must operate in such a way that they run with the least amount of system privilege needed to perform a specific function and that system access is granted on a need to know basis;

(2) 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;

(3) Information systems must be configured to the most restrictive mode consistent with operational requirements and IAW appropriate procedural guides from NIST and/or GSA to the greatest extent possible. Implemented configuration settings should be documented and enforced in all subsystems of the information system.

d. Remote access/end point security (Chapter 4.v)

(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 that checks 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 that fail this scan will not be
allowed access to the GSA network or any GSA IT resources;
(3) Only GSA GFE that is determined to be properly secured (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 security scans noted in paragraph b). 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 security scans noted in paragraph b).

e. PII. The following security requirements apply to the protection of PII (Chapter 4.w)

(1) If it is a business requirement to store PII on GSA user workstations or mobile
devices including, but not limited to notebook computers, USB drives, CD-
ROMs/DVDs, personal digital assistants, PII must be encrypted using a FIPS 140-
2 certified encryption module. An employee or contractor shall not physically
take PII from GSA facilities (including GSA managed programs housed at
contractor facilities under contract), or access remotely (i.e., from locations
other than GSA facilities), without written permission from the employee’s
supervisor, the data owner, and the IT system Authorizing Official. Approvals
shall be filed with the employee’s supervisor. This applies to electronic media
(e.g., laptops, USB drives), paper, and any other media (e.g., CDs/DVDs) that
may contain PII.
(2) PII shall be stored on network drives and/or in application databases with
proper access controls (i.e., User ID/password) and shall be made available
only to those individuals with a valid need to know.

f. Guest Wireless Access (Chapter 4, Paragraph 2.x)

(1) A GSA Guest Wireless Network has been established in the Regional and Central
Office Buildings to allow non-Government Furnished Equipment (GFE) access
only to the Internet and GSA resources that are available to the general public
(www.gsa.gov). It is intended to be a service for customers of the agency, as well
as vendors performing official business on site.
   a. Guest wireless accounts are not ENT accounts;
b. The user ID will change weekly;
c. The password is posted on InSite;
d. The password is changed monthly;
e. Guest wireless traffic will be subject to the same content filtering as traffic on the production network.

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

Chapter 5 of GSA Order CIO 2100.1 states:

a. Identification and authentication (Chapter 5, Paragraph 2.a)

All GSA systems must incorporate a proper user identification and authentication methodology. Refer to the GSA CIO-IT Security-01-01: Identification and Authentication Procedural Guide for additional details. For mobile devices, refer to Chapter 4.

(2) An authentication scheme using passwords as a credential must implement the following security requirements:

(c) Information systems must automatically lockout users after not more than ten (10) failed access attempts during a 30 minute time period. Accounts must remain locked for a minimum of 30 minutes for the next login prompt.

(12) All GSA workstation and mobile devices shall initiate a session lock after 15 minutes of inactivity. The session lock shall remain in effect until the user reestablishes access using appropriate identification and authentication.

(13) FIPS 199 Moderate and High impact systems shall automatically terminate temporary and emergency accounts after no more than ninety (90) days.

(14) FIPS 199 Moderate and High impact systems shall automatically disable inactive accounts after ninety (90) days.

(15) FIPS 199 Moderate and High impact systems shall automatically terminate:

(a) A remote access connection after thirty (30) minutes of inactivity;
(b) An Internet accessible application session after thirty (30) minutes of inactivity; or
(c) A non-interactive user session after thirty (30) – sixty (60) minutes of inactivity. Static web sites and long running operations (e.g., batch jobs) are not subject to this time limit.

NOTE: An AO, upon concurrence of the GSA CISO, may grant an exception to this requirement only if the system is technically unable to implement the requirement or an approved business justification and sufficient compensating controls have been implemented to reduce the risk to an acceptable level.

(17) FIPS 199 Moderate and High impact systems shall automatically terminate:
(a) A remote access connection after thirty (30) minutes of inactivity;
(b) An Internet accessible application session after thirty (30) minutes of
inactivity; or
(c) A non-interactive user session after thirty (30) – sixty (60) minutes of
inactivity. Static web sites and long running operations (e.g., batch jobs) are
not subject to this time limit.

b. Logical access controls (Chapter 5, Paragraph b)

    (1) All GSA systems must implement logical access controls to authorize or restrict
        the activities of users and system personnel to authorized transactions and
        functions;
    (2) Public users must be restricted to using designated public services;
    (3) Information system accounts must be managed for all systems, including
        establishing, activating, modifying, reviewing, disabling, and removing accounts.
        Reviews and validations of system users’ and staff users’ accounts shall be
        completed annually to ensure the continued need for system access;
    (4) 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;
    (5) 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.

        (a) 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, SaaS, mobile applications, and Google Apps Scripts;
        (b) OAuth 2.0 Access Scopes are used to limit the authorization granted to
            the relying service by the GSA.gov user. The Access Scopes listed below
            present risk to GSA.gov accounts and data and are prohibited unless
            integrated with websites, mobile apps, and SaaS Authorized to Operate
            by GSA and/or included in the GSA IT Standards Profile.

            1. **Access inbox and contacts information.** Allows view of email
                messages and settings.
            2. **Access personal information.** Allows manage of user calendars.
            3. **Act on behalf of user.** Allows view and modify but not delete user
                email.
            4. **Full data access.** Allows view and manage of files and documents in
                connecting users Google Drive.
            5. **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 your Google Drive.
            6. **Manage devices.** Administrator's scope to view and manage your
                mobile devices' metadata.
7. **Manage user activity.** Administrator’s scope to view users on your domain; manage org units in domain; view org units in domain; view and manage provisioning of users in domain; general domain API operations include managing a domain's language, organization name, max number of users; current number of users.

8. **Other.** Miscellaneous permissions.

9. **Payment information.** Read Google Wallet credentials from the production environment.

10. **Read only access to data and files.** “Read Only Access” to data and files.

11. **Access location information.** Google Map Data API - View your Google Maps engine data; Google FIT: Location.

(c) The OAuth 2.0 Access Scopes listed in the (CIO 2100.1 Ch. 5, Para. B., sub. 5c.) are authorized for integration with GSA.gov accounts with no restriction;

1. **Basic Info.** View your email address; View basic information about your account, including name, public profile URL, photo, gender, birthdate, country, language, and time zone.

2. **Limited access to data and Files.** Access Google+ features which are generally public.

(d) 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 may be restricted pending results of the OCISO review;

2. Internally developed scripts shall follow GSA naming conventions – GSA_2 Letter S/SO Designation_Script Name (e.g., GSA_IS_Script Name);

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

c. **Warning banners/system use notification message (Chapter 5, Paragraph d)**

(1) All internal GSA IT systems must display an approved warning banner to all users attempting to access GSA’s computer systems. The warning banner must read as follows:

```
**********************************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 are subject to disciplinary action including criminal prosecution.
```
d. **Remote access (Chapter 5, Paragraph e)**

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

   (1) Individuals other than GSA employees and contractor personnel are not allowed to use GSA furnished computers, GSA VPN connection, or a GSA provided or funded internet connection;
   (2) Users must not connect to other computers or networks via modem while simultaneously connected to the GSA network (i.e., no dialing outbound to your Internet Service Provider or allowing inbound calls to your computer while at the same time being connected to GSA’s network). However, accessing GSA’s network via the GSA-provided VPN software is allowed;
   (3) When using the GSA IT IPsec VPN, users must connect using only IP and must have the client firewall bound to all network adapters;
   (4) Allow remote access only with multifactor authentication where one of the factors is provided by a device separate from the computer gaining access. All remote access connections shall automatically terminate within 30 minutes of inactivity.

e. **Account Management (Chapter 5, Paragraph l)**

   (1) Request and approval routing in support of account management processes must assure:
      (a) All access requests require at least one supervisor approval. Access requests submitted directly from a user must not be accepted, regardless of position;
      (b) Users complete and send access requests to their supervisor or Contracting Officer Representative (COR), not directly to the Data or System Owner;
      (c) Access requests may be aggregated and managed by designated coordinators for efficiency;
      (d) Access requests are routed to the data or System Owner by a user’s supervisor, COR, ISSO, ISSM, director, or designated regional coordinator.

   (2) Authorizations supporting the account management processes must assure:
      (a) Supervisors are responsible for coordinating and arranging system access requests for all new or transferring employees and for verifying an individual’s need-to-know;
      (b) Data owners/system owners, with assistance from the designated ISSO, ensure system access is restricted to authorized users that have completed required background investigations, are familiar with internal security practices, and have completed requisite security and privacy awareness training programs, such as the annual Information Security &
Privacy Act training curriculum. System access authorizations must enforce job function alignment, separation of duties, and be based on the principle of need-to-know. Contractors with system access must utilize a gsa.gov e-mail account to conduct business with GSA.

(3) Establishment and activations supporting the account management processes must assure:
   (a) Data or system owner grants 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;
   (b) The delegation of user roles or permissions for applications, in particular those containing Personally Identifiable Information (PII) and/or sensitive financial data, must be compliant with the principles of least privilege, separation of duties, and need-to-know;
   (c) Accounts are created only upon receipt of valid access requests conforming to the GSA access request protocol.

(4) Update and modification of user accounts supporting account management processes must ensure:
   (a) Supervisors are responsible for coordinating and arranging system access modifications for personnel;
   (b) Users complete and send account update requests directly to his or her supervisor or COR, not directly to the Data or System Owner;
   (c) Update requests are aggregated and managed by designated regional coordinators for efficiency;
   (d) Update requests are routed to the Data or System Owner by a user’s supervisor, COR, director, or designated regional coordinator.

(5) Disabling and removal of user accounts supporting account management processes must ensure:
   (a) Supervisors are responsible for coordinating and arranging system access termination for all departing or resigning personnel;
   (b) Account removal is initiated by a user’s supervisor, COR, or through the review of the monthly OHRM separation list submitted by the OCISO;
   (c) Removal requests may be aggregated and managed by designated regional coordinators for efficiency;
   (d) Termination and transfer procedures must be incorporated into the authorization process for all information systems.

(6) User authorizations must be verified annually for all information systems;

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

(8) On a regular basis, data and system owners must inspect user access entitlements as needed to detect the following conditions that warrant termination, revocation, or suspension of account access:
(a) **Orphaned accounts.** An orphaned account is defined as a user account that has demonstrated, or is expected to demonstrate, an extensive period of idle time consistent with account abandonment.

1. FIPS 199 Moderate and High impact systems shall automatically disable inactive accounts after 90 days and shall automatically terminate temporary and emergency accounts after no more than 90 days;
2. Upon issuance of the CISO monthly separation reports, Data and System Owners must verify within 30 days that separated personnel no longer maintain access to GSA IT systems or resources.

(b) **Role conflicts.** Any accesses or permissions that clearly violate established separation of duties policies must be coordinated with the designated S/RO/R ISSO to correct or resolve conflicting role assignments;

(c) **Shared accounts.** Shared user accounts violate the principles of separation of duties and non-repudiation, and must be detected and suspended when discovered;

(d) **Suspension or revocations of GSA e-mail accounts.** Systems that require users to maintain an active e-mail account must suspend or revoke access for users whose e-mail credentials are no longer valid.

(9) **GSA Customer Affiliated Accounts (GACA)** are a means where any gsa.gov user can share collaboratively in a secure environment with non-GSA users not normally provided a gsa.gov email account. Procedures for setting up a GACA account by an affiliated customer of GSA can be found here [GACA Accounts](#). GACA accounts are not to be used by GSA employees, contractors or other users (detailee, interns, etc.) requiring regular/repeated access to the GSA network for GSA's Google domain to conduct business. If you have a question on the proper use of a GACA account or assistance in proper set up, please contact your local IT Manager or Regional ISSO.