



**IT Security Procedural Guide:
Identification and Authentication
(IA)
CIO-IT Security-01-01**

Revision 6
March 20, 2019

VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
Revision 1 - June 23, 2005				
1	Scott/Heard	Changes made throughout the document to reflect FISMA, NIST and GSA CIO P 2100.1 requirements.	Updated to reflect and implement various FISMA, NIST and GSA CIO P 2100.1 requirements.	Various
2	Scott/Heard	Changes throughout the document to correspond with revisions made to CIO-IT Security-01-09, CIO-IT Security-01-03 and CIO-IT Security-01-04.	Updated to reflect the correlation of the CIO-IT Security Guides; and to further express policy within them as stand-alone documents.	Various
Revision 2 - January 08, 2008				
1	Berlas	Changes made throughout the document to reflect FDCC password requirements.	OMB Memorandum M-07-11 mandates the implementation of FDCC configuration requirements.	Various
Revision 3 – June 22, 2010				
1	Berlas/Cook	Changes made throughout the document to reflect updates in governing policy and procedures, including, NIST SP 800-53 rev3, HSPD-12, OMB e-Authentication, and FDCC password requirements.	Updated to reflect and implement OMB, NIST, and GSA CIO P 2100.1 requirements.	Various
Revision 4 – April 17, 2015				
1	Graham	Changes to the Revision number and date of the document. Updated Cover Page, Sections 1.2, 2-4, and Appendices to reflect CIO 2100.1 and GSA guidance.	Updated sections to provide current references, current policy statements and methodologies.	All
2	Heard	Included references from the IT security Program Plan.	Various	Various
Revision 5 – May 5, 2017				
1	Feliksa/Dean /Klemens	Changes made throughout the document to align with current OMB, NIST, and GSA policies.	Updated to align with the current version of GSA CIO 2100.1, format to latest guide structure and style, revise guidance to current GSA policies and processes.	Throughout
Revision 6 – March 20, 2019				
1	Dean/ Klemens	Updated format and NIST SP 800-53 control parameters, added a section on SCRM, included EO 13800 and NIST Cybersecurity Framework.	Biennial update.	Throughout

Approval

IT Security Procedural Guide: Identification and Authentication, CIO-IT Security-01-01, Revision 6 is hereby approved for distribution.

3/20/2019

X Bo Berlas

Bo Berlas
Acting GSA Chief Information Security Officer
Signed by: General Services Administration

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

Table of Contents

1	Introduction	1
1.1	Purpose.....	2
1.2	Scope	2
1.3	Policy.....	3
1.4	References	5
2	Roles and Responsibilities.....	7
2.1	Authorizing Official (AO).....	7
2.2	Information Systems Security Manager (ISSM).....	7
2.3	Information System Security Officer (ISSO).....	7
2.4	System Owners	7
2.5	Data Owners	8
2.6	Authorized Users of IT Resources	8
2.7	System/Network Administrators.....	8
2.8	Supervisors	9
3	Implementation Guidance for IA Controls	10
3.1	IA-1: Identification and Authentication Policy and Procedures	10
3.2	IA-2: Identification and Authentication (Organizational Users)	11
3.3	IA-3: Device Identification and Authentication	14
3.4	IA-4: Identifier Management	14
3.5	IA-5: Authenticator Management	16
3.6	IA-6: Authenticator Feedback.....	21
3.7	IA-7: Cryptographic Module Authentication	21
3.8	IA-8 Identification and Authentication (Non-Organizational Users)	22
4	Identification and Authentication and Supply Chain Risk Management	23
4.1	IA-1 Identification and Authentication Policy and Procedures (ICT SCRM).....	23
4.2	IA-2 Identification and Authentication (Organizational Users) (ICT SCRM)	24
4.3	IA-4 Identifier Management (ICT SCRM)	24
4.4	IA-5 Authenticator Management (ICT SCRM).....	25
4.5	IA-8 Identification and Authentication (Non-Organizational Users) (ICT SCRM)	25
	Appendix A: Definitions	26
	Table 1-1: NIST SP 800-53 Control to CSF Mapping	2

Note: I&A and IA are used throughout this guide. IA is used when referring to NIST SP 800-53 security controls or in relation to those controls. I&A is used as an acronym for identification and authentication and when referring to processes, features, or mechanisms used to implement user identification and user authentication.

1 Introduction

Identification and Authentication (I&A) is critical to securing agency information and information technology (IT) assets. Account Management deals with the creation and management of information systems accounts, I&A focuses on assignment and management of accounts to users and devices. An effective I&A program is often the first line of defense for protecting IT assets and data in that it provides a secure process for the assignment and management of user and device accounts as well as establishing strong password policies to protect General Services Administration (GSA) information systems from unauthorized access and use.

The mechanisms associated with I&A, when effectively applied, ensure that individuals or devices accessing or connecting to GSA's IT resources are indeed who they represent themselves to be. The most commonly known I&A mechanisms are usernames and passwords. GSA has implemented multi-factor authentication (MFA) with smartcards at the desktop as required by GSA Order CIO 2100.1, "*GSA Information Technology (IT) Security Policy*." The use of MFA and to a lesser extent, unique account names combined with strong, well-constructed passwords help to ensure the confidentiality of GSA information and the integrity of IT resources. The I&A principles and practices described in this guide and guidance regarding the IA control family are based on the following documents:

- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, "*Security and Privacy Controls for Federal Information Systems and Organizations*"
- NIST SP 800-63-3, "*Digital Identity Guidelines*"
- NIST SP 800-63A, "*Digital Identity Guidelines: Enrollment and Identity Proofing*"
- NIST SP 800-63B, "*Digital Identity Guidelines: Authentication and Lifecycle Management*"
- NIST SP 800-63C, "*Digital Identity Guidelines: Federation and Assertions*"

Every GSA IT system must follow the IA practices identified in this guide. Any deviations from the security requirements established in GSA Order CIO 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, or other conditions not following GSA policies and standards must be submitted using the [Security Deviation Request Google Form](#). Deviations must also be documented using the Acceptance of Risk (AoR) process defined in GSA CIO-IT Security-06-30, "*Managing Enterprise Risk*," including a date of resolution to comply.

Executive Order (EO) 13800, "*Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*" requires all agencies to use "*The Framework for Improving Critical Infrastructure Cybersecurity (the Framework)* developed by the National Institute of Standards and Technology (NIST) or any successor document to manage the

agency's cybersecurity risk." This NIST document is commonly referred to as the Cybersecurity Framework (CSF).

The CSF focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes. The core of the CSF consists of five concurrent and continuous Functions—Identify (ID), Protect (PR), Detect (DE), Respond (RS), and Recover (RC). The CSF complements, and does not replace, an organization's risk management process and cybersecurity program. GSA uses NIST's Risk Management Framework from NIST SP 800-37, Revision 1, *"Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach."* Table 1-1 provides a mapping of the NIST SP 800-53 IA controls to CSF Category Unique Identifiers. The following CSF categories are aligned with NIST's IA controls.

- Identify – Governance (ID.GV)
- Protect – Access Control (PR.AC)

Table 1-1: NIST SP 800-53 Control to CSF Mapping

NIST SP 800-53 Control	CSF Category Unique Identifier Codes
IA-1	ID.GV-1, ID.GV-3, PR.AC-1, PR.AC-6, PR.AC-7
IA-2	PR.AC-1, PR.AC-6, PR.AC-7
IA-3	PR.AC-1, PR.AC-7
IA-4	PR.AC-1, PR.AC-6, PR.AC-7
IA-5	PR.AC-1, PR.AC-6, PR.AC-7
IA-6	PR.AC-1
IA-7	PR.AC-1
IA-8	PR.AC-1, PR.AC-6, PR.AC-7

1.1 Purpose

The purpose of this guide is to provide guidance for the IA security controls identified in NIST SP 800-53 and I&A requirements specified in CIO 2100.1. This procedural guide provides GSA Federal employees and contractors with significant security responsibilities, as identified in CIO 2100.1, and other IT personnel involved in implementing I&A mechanisms, the specific procedures and processes they are to follow for systems under their purview.

1.2 Scope

The requirements outlined within this guide apply to all GSA Federal employees and contractors involved in I&A implementations for GSA information systems. All GSA systems must adhere to the requirements and guidance provided with regard to I&A features, mechanisms, and methods.

1.3 Policy

CIO 2100.1 Chapter 4, Policy for Protect Function, Section 1, Identity Management, Authentication and Access Control establishes the following policies for identification and authentication required for GSA information systems.

b. All users issued GFE are required to log into the workstation using a GSA issued [Personal Identity Verification] PIV credential. The following groups of users are exempt from this requirement:

(1) A Federal employee on detail to GSA issued a PIV from the employee's assigned Agency.

(2) Any employee or contractor expected to be employed for less than 180 days and not issued a PIV.

(3) Any person with a disability that does not allow the individual to utilize a PIV card and laptop.

(4) Any user with a PIV that is lost, forgotten at home, or damaged in any way, may contact the IT Service Desk (ITSD) to request a temporary exception to the above requirement, not to exceed forty-five (45) days.

c. Systems with users who are agency business partners or the general public, and who register or log into the system, must accept credentials issued by identity providers who have been certified by federally approved Trust Framework Providers.

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

aaa. User IDs shall be unique to each authorized user.

bbb. Authentication schemes for all systems must utilize MFA using two or more types of identity credentials (e.g., passwords, SAML 2.0 biometrics, tokens, smart cards, one time passwords) as approved by the AO and IAW the security requirements in the subparagraphs of this paragraph. Systems following the Low Impact SaaS process (GSA CIO-IT Security-16-75) are exempt from this requirement.

(1) Privileged accounts must use MFA when accessing any system via a network.

(2) Non-privileged accounts must use MFA when accessing a FIPS 199 Moderate or High level system via a network.

ccc. An authentication scheme using passwords as a credential must implement the following security requirements:

(1) Password length:

(a) Passwords for accounts used to access operating systems (workstations and servers) must contain a minimum of sixteen (16) characters.

- (b) Passwords for systems/other accounts (e.g., service, application) must contain a minimum of eight (8) characters.*
- (c) Passwords for all mobile devices such as GSA approved smart phones, iPads, and tablets must be a minimum of 6 characters. The six-character password requirement also applies to personal mobile devices accessing GSA data or systems.*
- (2) Password complexity:*
- (a) Systems not implementing a password solution rejecting unacceptable passwords, as described below, must require a combination of letters, numbers, and special characters.*
- (b) Systems implementing a password solution rejecting unacceptable passwords, as described below, do not need to enforce password complexity requirements.*
- 1. The password solution must reject unacceptable passwords (e.g., commonly used, expected, or compromised). For example, the password solution should reject previously breached passwords, dictionary words, repetitive or sequential characters (e.g., 'aaaaaaaa', '1234abcd', '1qaz2wsx'), context sensitive words, such as the name of the service/website, the username, and derivatives of them.*
 - 2. Password solutions must be approved by the CISO and the AO.*
- (3) Password expiration:*
- (a) Systems rejecting passwords based on a password solution, as described above, only need to force password changes when a password is compromised or forgotten.*
- (b) Systems not rejecting passwords based on password solution, as described above, must require passwords to be changed every 90 days and when a password is compromised or forgotten.*
- (4) Passwords must not be stored in forms (i.e., Windows dialog boxes, web forms, etc.).*
- (5) All default passwords on network devices, databases, operating systems, etc. must be changed.*
- (6) Password distribution:*
- (a) Passwords must never be distributed via regular mail or interoffice mail.*
 - (b) User IDs and passwords must never be distributed together.*
 - (c) User IDs and passwords must be distributed via separate emails or channels (e.g., email, text, telephone).*
 - (d) Passwords used for authentication (other than default or one time use passwords) must not be transmitted in the clear.*

- (7) Users must be authenticated before resetting or distributing a password.
- (8) One time use passwords must expire in:
- (a) Two (2) minutes if based on a real-time clock;
 - (b) Ten (10) minutes if sent by means other than physical mail;
 - (c) Seven (7) days if sent to a postal address of record;
 - (d) Twenty-one (21) days if an exception is granted to accommodate an address of record outside the direct reach of the U.S. Postal Service.
- (9) Password managers are permitted as long as they are listed on the GSA IT Standards List with a Status of Approved or Exception.

ddd. Authentication methods for applications and systems may use the authentication mechanisms provided by the major information system if deemed appropriate by the AO.

eee. E-commerce and publicly accessible systems must incorporate identification and authentication mechanisms commensurate with their security risks and business needs and may differ from the security requirements set forth by this policy. In such cases the identification and authentication mechanisms must be approved by the AO in writing and concurred by the OCISO.

CIO 2100.1 Chapter 4, Policy for Protect Function, Section 3, Data Security, establishes the following policy statement.

f. Web sites (internal and public) with logon functions, must implement TLS encryption with a FIPS 140-2 validated encryption module. SSL/TLS implementation must be IAW GSA CIO-IT Security-14-69: SSL/TLS Implementation Guide.

1.4 References

Note: GSA updates its IT security policies and procedural guides on independent biennial cycles which may introduce conflicting guidance until revised guides are developed. In addition, many of the references listed are updated by external organizations which can lead to inconsistencies with GSA policies and guides. When conflicts or inconsistencies are noticed, please contact ispcompliance@gsa.gov for guidance.

Federal Laws and Regulations:

- [EO 13800](#), "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure"

Federal Guidance:

- [CSF, Version 1.1](#), "Framework for Improving Critical Infrastructure Cybersecurity"
- [Federal Information Processing Standards \(FIPS\) Publication \(PUB\) 140-2](#), "Security Requirements for Cryptographic Modules"
- [FIPS PUB 199](#), "Standards for Security Categorization of Federal Information and Information Systems"

- [FIPS PUB 201](#), “Personal Identity Verification (PIV) of Federal Employees and Contractors”
- [Homeland Security Presidential Directive 12 \(HSPD-12\)](#), “Policy for a Common Identification Standard for Federal Employees and Contractors”
- [NIST SP 800-37, Revision 1](#), “Guide for Applying the Risk Management Framework to Federal Information Systems”
- [NIST SP 800-53, Revision 4](#), “Security and Privacy Controls for Federal Information Systems and Organizations”
- [NIST SP 800-63-3](#), “Digital Identity Guidelines”
- [NIST SP 800-63A](#), “Digital Identity Guidelines: Enrollment and Identity Proofing”
- [NIST SP 800-63B](#), “Digital Identity Guidelines: Authentication and Lifecycle Management”
- [NIST SP 800-63C](#), “Digital Identity Guidelines: Federation and Assertions”
- [NIST SP 800-161](#), “Supply Chain Risk Management Practices for Federal Information Systems and Organizations”

GSA Guidance:

- [GSA Order CIO 2100.1](#), “GSA Information Technology (IT) Security Policy”

The guidance documents below are available on the [GSA IT Security Procedural Guides](#) InSite page.

- CIO-IT Security-06-30, “Managing Enterprise Risk”
- CIO-IT Security-09-48, “Security and Privacy Requirements for IT Acquisition Efforts”
- CIO-IT Security-18-90, “Information Security Program Plan”
- CIO-IT Security-14-69, “SSL/TLS Implementation”
- CIO-IT Security-18-88, “Moderate Impact Software as a Service (MiSaaS) Security Authorization Process”

2 Roles and Responsibilities

There are many roles associated with implementing effective I&A policies and procedures. The roles and responsibilities provided in this section have been extracted or paraphrased from CIO 2100.1 or summarized from GSA and Federal guidance. The responsibilities listed in this guide are focused on I&A, a complete set of GSA security roles and responsibilities can be found in CIO 2100.1. Throughout this guide, specific processes and procedures for implementing NIST's IA controls are described.

2.1 Authorizing Official (AO)

Responsibilities include the following:

- Reviewing and approving security safeguards of information systems (including IA controls) and issuing ATO approvals for each information system under their purview based on the acceptability of the security safeguards of the system (risk-management approach).
- Providing support to the ISSM and ISSO of record for each information system under their purview.

2.2 Information Systems Security Manager (ISSM)

Responsibilities include the following:

- Verifying systems under their purview have appropriately addressed NIST SP 800-53 IA controls.
- Coordinating with the AO, System Owner, ISSOs, and OCISO Directors, as necessary, regarding IA control implementation and compliance with NIST and GSA requirements.

2.3 Information System Security Officer (ISSO)

Responsibilities include the following:

- Ensuring necessary IA security controls are in place and operating as intended.
- Ensuring the user identification and authentication scheme used in systems under their purview are administered as intended, including reviewing system role assignments to validate compliance with principles of least privilege.
- Assisting System Owners and Data Owners in verifying user accounts are only issued when authorized, verified annually, and terminated when no longer needed.

2.4 System Owners

Responsibilities include the following:

- Ensuring necessary NIST SP 800-53 IA security controls are in place and operating as intended.

- Conducting annual reviews and validation of system users' accounts to ensure the continued need for access to a system and verify users' authorizations (rights/privileges).
- 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.

2.5 Data Owners

Responsibilities include the following:

- Coordinating with System Owners and Custodians to ensure the data each system processes has necessary NIST SP 800-53 IA Security controls in place and operating as intended.
- 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 awareness training programs (e.g., the annual IT Security Awareness Training and Sharing Information in a Collaborative Environment training).
- Reviewing access authorization listings and determining whether they remain appropriate at least annually.
- Ensuring information systems that allow authentication of users for the purpose of conducting Government business electronically complete a Digital Identity Acceptance Statement for digital transactions resulting in an assurance level classification IAW [NIST SP 800-63-3](#), Digital Identity Guidelines.

2.6 Authorized Users of IT Resources

Responsibilities include the following:

- Ensuring that adequate protection is maintained on their workstation, including not sharing passwords with any other person and logging out, locking, or enabling a password protected screen saver, and removing their PIV card before leaving their workstation.
- Utilizing assigned privileged access rights (e.g., administrator, power user, database administrator, web site administrator, etc.) to a computer based on need-to-use (i.e., using accounts with those privileges only when the privileges are required to complete an action).

2.7 System/Network Administrators

Responsibilities include the following:

- Ensuring the appropriate security requirements are implemented consistent with GSA IT security policies and hardening guidelines.

- Utilizing privileged access rights (e.g., “administrator,” “root,” etc.) to a computer based on a need-to-use basis (i.e., using accounts with those privileges only when the privileges are required to complete an action).
- Ensuring system/network administrators have separate administrator and user accounts, if applicable (e.g., Microsoft Windows accounts). A normal user account should be used unless administrator rights are required to perform a job function.
- Utilizing GSA provided MFA to ensure strong authentication.

2.8 Supervisors

Responsibilities include the following:

- Conducting annual review and validation of staff user accounts to ensure the continued need for access to a system.
- Coordinating and arranging system access requests for all new or transferring employees and verifying an individual’s need to know (authorization)
- Coordinating and arranging system access termination for all terminating or transferring personnel.
- Coordinating and arranging system access modifications for personnel.

3 Implementation Guidance for IA 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 the identification and authentication processes, features, and mechanisms for GSA information systems and data. The GSA implementation guidance stated for each IA control applies to personnel and/or the systems operated on behalf of GSA. Any additional instructions/requirements for contractor systems will be included in the additional contractor system considerations portion of each control section.

IA-1, Identification and Authentication 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 IA-2 to IA-8 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. CIO-IT Security-18-90, "Information Security Program Plan" describes the GSA enterprise-wide inheritable common and hybrid controls and outlines the responsible party for implementing them.

3.1 IA-1: Identification and Authentication Policy and Procedures

Control: The organization:

- a. Develops, documents, and disseminates to [*personnel with IT security responsibilities as defined in GSA CIO Order 2100.1*]:
 1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and
- b. Reviews and updates the current:
 1. Identification and Authentication policy [*biennially*]; and
 2. Identification and Authentication procedures [*biennially*].

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

Common Control Implementation:

I&A policies and procedures is a common control provided by the OCISO Policy and Compliance Division (ISP). I&A Policy is included in GSA Order CIO 2100.1, "GSA Information Technology (IT) Security Policy," Chapter 5, Policy on Technical Controls. The policy states: "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." CIO 2100.1 contains a number of other specific policies regarding I&A technologies. As stated in the policy, GSA OCISO ISP has also defined agency-wide I&A procedures in CIO-IT Security-01-01. GSA's security policy and procedural guides are disseminated via the IT Security InSite [page](#).

CIO 2100.1 and CIO-IT Security-01-01 are reviewed and updated at least biennially.

Additional Contractor System Considerations:

Vendors/contractors may defer to the GSA policy and guide or implement their own I&A policies and procedures which comply with GSA's requirements with the approval of the AO.

3.2 IA-2: Identification and Authentication (Organizational Users)

Control: The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

Control Enhancements:

- (1) Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts. The information system implements multifactor authentication for network access to privileged accounts.
- (2) Identification and Authentication (Organizational Users) | Network Access to Non-Privileged Accounts. The information system implements multifactor authentication for network access to non-privileged accounts.
- (3) Identification and Authentication (Organizational Users) | Local Access to Privileged Accounts. The information system implements multifactor authentication for local access to privileged accounts.
- (4) Identification and Authentication (Organizational Users) | Local Access to Non-Privileged Accounts. The information system implements multifactor authentication for local access to non-privileged accounts.
- (8) Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts - Replay Resistant. The information system implements replay-resistant authentication mechanisms for network access to privileged accounts.
- (9) Identification and Authentication (Organizational Users) | Network Access to Non-Privileged Accounts – Replay Resistant. The information system implements replay-resistant authentication mechanisms for network access to non-privileged accounts.
- (11) Identification and Authentication (Organizational Users) | Remote Access - Separate Device. The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [GSA S/SO or Contractor recommended and GSA AO approved strength of mechanism requirements].
- (12) Identification and Authentication (Organizational Users) | Acceptance of PIV Credentials. The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials.

GSA Implementation Guidance: Control IA-2 and enhancements IA-2(1) and (12) are applicable at all FIPS 199 levels. In addition, control enhancements IA-2(2), (3), (8), and (11) are applicable at the FIPS 199 Moderate and High levels. Control enhancements IA-2(4) and (9) are also applicable at the FIPS 199 High Level.

The focus of IA-2 is to implement unique identification and authentication of organizational users to the level of an individual/process. This control is not concerned with privileges, but is concerned with binding the identity (user or process acting on behalf of user) to the identification/authentication process. This control is applicable to all components of a system.

Organizational users include organizational employees or individuals who the organization deems to have the equivalent status of employees (e.g., contractors, guest researchers, other authorized individuals, etc.). Examples of how the authentication of user identities is accomplished are: passwords, tokens, Security Assertion Markup Language (SAML) 2.0, biometrics, one-time passwords, smart cards or in the case of MFA, some combination thereof. In addition to identifying and authenticating organizational users at the information system level (i.e., at logon), identification and authentication mechanisms are employed at other components of the information system (e.g., operating system, database, application), when necessary, to uniquely identify users. The outcome of this control is that an effective process has been implemented in which users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in control AC-14, Permitted Actions without Identification or Authentication. Every function that is not mentioned in AC-14 must have an identification and authentication capability and must be addressed in the control discussion. Unique identification of individuals in group accounts may need to be considered for detailed accountability of activity.

Digital Identity Acceptance Statement:

Any GSA system providing digital services/online transactions over an open network (e.g., the Internet) that requires authentication or identity proofing must complete a Digital Identity Acceptance Statement. A GSA Digital Identity Acceptance Statement template is available on the IT Security Forms InSite [page](#). The template assists in determining a system's Identity Assurance Level (IAL), Authentication Assurance Level (AAL), and optionally, a Federation Assurance Level (FAL), based on guidance in the NIST SP 800-63 series on digital identities.

Organizational Access:

Access to organizational information systems is defined as either local or network.

- **Local access** is any access to an organizational information system by a user (or process acting on behalf of a user) where such access is obtained by direct connection without the use of a network.
- **Network access** is any access to an organizational information system by a user (or process acting on behalf of a user) where such access is obtained through a network connection. Remote access is a type of network access which involves communication through an external network (e.g., the Internet). Internal networks include local area networks, wide area networks, and virtual private networks that are under the control of the organization. For a virtual private network (VPN), the VPN is considered an internal network if the organization establishes the VPN connection between organization-controlled endpoints in a manner that does not require the organization to depend on any external networks across which the VPN transits to protect the

confidentiality and integrity of information transmitted. Identification and authentication requirements for information system access by other than organizational users are described in IA-8.

FIPS 140-2 Validated Encryption Modules:

Per GSA's IT Security Policy, web sites (internal and public) with logon functions, must implement TLS encryption with a FIPS 140-2 validated encryption module. CIO-IT Security-14-69, "SSL/TLS Implementation," provides specific requirements and implementation details. Validated FIPS 140-2 Cryptographic Modules can be found by using the Advanced Search Type function on NIST's Cryptographic Module Validation Program and selecting "140-2" as the Standard and "Active" as the Validation Status at the following URL.

<https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search>

Inheritance:

The requirements for IA-2 may be fully satisfied as a common control or partially satisfied as a hybrid control if I&A processes for all individuals (e.g., employees, contractors, guest researchers, and other authorized individuals) and system/service accounts are provided by GSA's Active Directory infrastructure (GSA Enterprise Infrastructure Operations [EIO] system). The GSA EIO system administers the I&A of individuals (users) in the GSA network and enables control of their access to system resources within the GSA network by leveraging user rights and access controls against a unique user identity. I&A of users is achieved through the integration of GSA applications with the Microsoft Active Directory Services (AD) architecture, the HSPD-12 Logical Access System, and Public Key Infrastructure (PKI).

If a system implements separate I&A at other component levels (i.e., not leveraging the I&A of users from GSA's AD implementation—at logon), then the I&A mechanisms at the component levels (e.g., operating system, database, application) must also meet the IA controls required based on the system's FIPS 199 level. Details on how I&A is implemented in GSA's AD implementation is documented in the most current GSA EIO System Security Plan.

Solutions that satisfy GSA's multifactor authentication requirements include:

- PIV Cards
- PIV Derived SAML, OIDC, OAUTH
- TOTP – e.g., Google Authenticator, Authy
- HTOP
- FIDO
- WebAuth

Additional Contractor System Considerations:

Contractor systems not utilizing GSA I&A standards must provide the system's I&A settings to GSA for review and approval by the AO and concurrence by the GSA CISO. Vendor/contractor

systems must comply with the control IAW the guidance above and the AO must approve contractor recommended parameters.

3.3 IA-3: Device Identification and Authentication

Control: The information system uniquely identifies and authenticates [*GSA S/SO or Contractor recommended and AO approved specific and/or types of devices*] before establishing a [*local, remote, or network*] connection.

GSA Implementation Guidance: Control IA-3 is applicable at the FIPS 199 Moderate and High levels.

The IA-3 control focus is the equivalent of the IA-2 control focus for unique I&A for individuals, but applied to defined devices. Control discussions must identify the specific devices or device types for which I&A is required before establishing connections to an information system; and the information system only establishes connections after it has verified the unique identity and that identity is authenticated for the defined devices.

The devices requiring unique I&A may be defined by type, by specific device, or by a combination of type and device as deemed appropriate. The information system typically uses either shared known information (e.g., Media Access Control [MAC] or Transmission Control Protocol/Internet Protocol [TCP/IP] addresses) for identification or an organizational authentication solution (e.g., IEEE 802.1x and Extensible Authentication Protocol [EAP], Radius server with EAP-Transport Layer Security [TLS] authentication, Kerberos, etc.) to identify and authenticate devices on local and/or wide area networks. The required strength of the device authentication mechanism will be determined by the FIPS 199 security categorization of the information system.

Additional Contractor System Considerations:

Vendor/contractor systems must comply with the control IAW the guidance above and the AO must approve contractor recommended parameters.

3.4 IA-4: Identifier Management

Control: The organization manages information system identifiers by:

- a. Receiving authorization from [*personnel with identifier assignment authorization as defined in GSA CIO Order 2100.1*] to assign an individual, group, role or device identifier;
- b. Selecting an identifier that uniquely identifies an individual, group, role or device;
- c. Assigning the identifier to the intended individual, group, role or device;
- d. Preventing reuse of identifiers for [*GSA S/SO or Contractor recommended and AO approved time period*]; and
- e. Disabling the identifier after [*a period of inactivity of 90 days for user level accounts, GSA S/SO or Contractor recommended and AO approved period of inactivity for non-user level accounts*].

GSA Implementation Guidance: Control IA-4 is applicable at all FIPS 199 levels.

This control addresses the authorization, creation, and management of user and device identifiers (accounts/names). Where IA-2 focused on uniquely identifying and authenticating users (and processes acting on the behalf of users), IA-4 focuses on the procedures and processes that have been established by the organization for managing identifiers for individuals, groups, roles, and devices. This control is associated with AC-2, Account Management, and serves an integral part in overall management and protection of user and device identifiers/accounts through the implementation of processes to support the requirements stated in the control objectives.

Successful implementation of this control will consist of the following processes/procedures:

- **Authorization to issue a user account from an appropriate organization official.**
Approval by at least one supervisor must be received prior to an account being issued. The authorization process begins when a manager or supervisor submits an account request for a new GSA employee or contractor. This request is reviewed by an authorized GSA official who must sign off on the request in order for an account to be created and issued. In addition, GSA requires annual reviews of accounts for re-authorization. All user accounts must be reviewed annually by the System Owner, Program Manager, and/or ISSO to ensure active accounts are still required for authorized personnel.
- **Creation of unique names for each user or device account.**
GSA uses several naming schemes in accordance with the account types and functions.

Non-administrative user accounts (Long Name Accounts) use an individual's full name as the identifier. Most commonly, users are assigned long name accounts for day-to-day business needs and have no administrative rights or permissions assigned to them. These accounts are most commonly used in naming Active Directory accounts.

Administrative user accounts (Short Name Accounts) are named to uniquely identify the individual and/or role they serve.

Common device account identifiers include media access control (MAC) or Internet protocol (IP) addresses, or device-unique token identifiers. Network enabled devices, including desktop and laptop computers are also assigned unique identifiers.

Default accounts such as Administrator and Guest are not allowed on GSA IT resources, and must be renamed.
- **Verification of user identity prior to issuance of an account.**
Employees and contractors must submit to a background investigation and employment suitability review, prior to being granted user accounts to access GSA networks and IT resources.
- **Issuing the account to the intended party.**

GSA accounts are uniquely assigned and identifiable to individual employees and contractors. All service accounts should be assigned to an individual and those individuals made responsible, via position description or performance measures, for the management, use, and protection of the authentication credentials associated with a particular service account.

- **Defining within the security plan, explicitly or by reference, the time period of inactivity after which a user account is to be disabled.**

GSA System Owners and ISSO's must comply with GSA parameters provided for controls IA-4 and AC-2(2) and (3), and document within their respective system security plans the specific time period of inactivity whereby an account is to be disabled. Administrative accounts are required to be disabled immediately upon transfer or termination of the account holder.

- **Preventing the reuse of user accounts.**

GSA requires non-administrative user accounts to be uniquely identifiable to an assigned user, and not to be reused or shared by any other party.

- **Disabling the account after the organization-defined time period of inactivity.**

All GSA systems must disable or terminate user level accounts after 90 days of inactivity. Non-user level accounts (device, token, smart cards, etc.) are deferred to the system (GSA S/SO organization) for determination. The setting must be approved by the GSA Authorizing Official before implementation.

Additional Contractor System Considerations:

Vendor/contractor systems must comply with the control IAW the guidance above and the AO must approve contractor recommended parameters.

3.5 IA-5: Authenticator Management

Control: The organization manages information system authenticators by:

- a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;
- b. Establishing initial authenticator content for authenticators defined by the organization;
- c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
- d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
- e. Changing default content of authenticators prior to information system installation;
- f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;
- g. Changing/refreshing authenticators [*per maximum lifetime specified in IA-5 (1)(d)*];
- h. Protecting authenticator content from unauthorized disclosure and modification;

- i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and
- j. Changing authenticators for group/role accounts when membership to those accounts changes.

Control Enhancements:

- (1) Authenticator Management | Password-Based Authentication. The information system, for password-based authentication:
 - (a) Enforces minimum password complexity of [
 - (1) *Password length.*
 - (a) *Passwords for accounts used to access operating systems (workstations and servers) must contain a minimum of sixteen (16) characters.*
 - (b) *Passwords for systems/other accounts (e.g., service, application) must contain a minimum of eight (8) characters.*
 - (c) *Passwords for all mobile devices such as GSA approved smart phones, iPads, and tablets must be a minimum of 6 characters. The six-character password requirement also applies to personal mobile devices accessing GSA data or systems.*
 - (2) *Password complexity.*
 - (a) *Systems not implementing a password solution rejecting unacceptable passwords, as described below, must require a combination of letters, numbers, and special characters.*
 - (b) *Systems implementing a password solution rejecting unacceptable passwords, as described below, do not need to enforce password complexity requirements.*
 1. *The password solution must reject unacceptable passwords (e.g., commonly used, expected, or compromised). For example, the password solution should reject previously breached passwords, dictionary words, repetitive or sequential characters (e.g., 'aaaaaaaa', '1234abcd', '1qaz2wsx'), context sensitive words, such as the name of the service/website, the username, and derivatives of them.*
 2. *Password solutions must be approved by the CISO and the AO.]*
 - (b) Enforces at least the following number of changed characters when new passwords are created: [at least 1 or GSA S/SO or Contractor recommended number to be approved by the GSA AO];
 - (c) Stores and transmits only cryptographically-protected passwords;
 - (d) Enforces password minimum and maximum lifetime restrictions of [
 - Password expiration.*
 - (a) *Systems rejecting passwords based on a password solution, as described above, only need to force password changes when a password is compromised or forgotten.*
 - (b) *Systems not rejecting passwords based on password solution, as described above, must require passwords to be changed every 90 days and when a password is compromised or forgotten.*

One time use passwords must expire in

1. *Two (2) minutes if based on a real-time clock;*
 2. *Ten (10 minutes if sent by means other than physical mail;*
 3. *Seven (7) days if sent to a postal address of record;*
 4. *Twenty-one (21) days if an exception is granted to accommodate an address of record outside the direct reach of the U.S. Postal Service.];*
- (e) Prohibits password reuse for [24] generations; and
- (f) Allows the use of a temporary password for system logons with an immediate change to a permanent password.
- (2) Authenticator Management | PKI-Based Authentication. The information system, for PKI-based authentication:
- (a) Validates certifications by constructing and verifying certification path to an accepted trust anchor including checking certificate status information;
 - (b) Enforces authorized access to the corresponding private key;
 - (c) Maps the authenticated identity to the account of the individual or group; and
 - (d) Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.
- (3) Authenticator Management | In-Person or Trusted Third-Party Registration. The organization requires that the registration process to receive [*multifactor authenticator tokens and passwords*] be conducted [*in person*] before [*a GSA approved registration authority*] with authorization by [*a GSA authorized official*].
- (7) Authenticator Management | No Embedded Unencrypted Static Authenticators. The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.
- (11) Authenticator Management | Hardware Token-Based Authentication. The information system, for hardware token-based authentication, employs mechanisms that satisfy [*HSPD-12 Smart Cards token quality requirements*].

GSA Implementation Guidance: Control IA-5 and enhancements IA-5 (1) and (11) are applicable at all FIPS 199 levels. Control enhancements IA-5 (2) and (3) are also applicable at the FIPS 199 Moderate and High levels. Control enhancement IA-5(7) is only applicable for MiSaaS systems using CIO-IT Security-18-88 for their A&A.

Note: Information in this guide regarding the allowed methods for distribution of passwords and Personal Identification Numbers (PINs) is a change to existing policy and procedure. Systems, applications, or processes that rely on methods that are no longer allowed must develop a plan to transition to an allowed method by September 30, 2019. CIO 2100.1, “GSA IT Security Policy,” will be updated to reflect these changes during its next revision cycle.

Initial Password Creation and Distribution:

A secure method for initial distribution of passwords and PINs should be documented in the system security plan and implemented for each IT resource. The administrator can create the account and an initial strong password (randomly chosen from a large space), provide it to the user, and instruct the user to use the password only for an initial login. The initial password

should be set to expire at first use. The user must be instructed to select a proper password based upon GSA's password guidelines. For especially sensitive applications, consider providing initial authentication information over the telephone after verifying the individual's identity.

In addition to the requirements specified in the control parameters for IA-5 and its enhancements, the following password policies/restrictions apply.

Password Policies/Restrictions:

- All default passwords on network devices, databases, operating systems, etc. must be changed.
- Passwords (and PINs) must never be sent via e-mail, regular mail, or interoffice mail.
- Password distribution:
 - Password/PINs may only be distributed via Short Message Service (SMS) to registered phone numbers and registered devices based on a documented, approved risk analysis decision.
 - User IDs and passwords must never be distributed together.
 - User IDs and passwords must be distributed via separate channels when not performed in person.
 - Passwords used for authentication must not be transmitted in the clear.
- To protect passwords, web sites (internal and public) with logon functions, must implement TLS encryption with a FIPS 140-2 validated encryption module.

Solutions that do not expose a user's password PIN in transit that meet GSA's requirements include:

- PIV Cards
- PIV Derived SAML, OIDC, OAUTH
- TOTP – e.g., Google Authenticator, Authy
- HTOP
- FIDO
- WebAuth

Password Administration:

- **Disable/change all default accounts and passwords.**
Most operating systems and applications including databases install with default accounts and passwords, some of which have critical system privileges. Disabling and changing all default accounts and passwords will prevent most scripted attacks and will delay more advanced manual attacks on a system.
- **Disable user accounts as quickly as possible when the user is no longer authorized resource access.**
Delete an account once files associated with an account have been reviewed and reassigned or removed;
- **Change passwords when a compromise is suspected.**

An automated password system should allow the administrator to delete or replace a password, and it should have the capability to maintain a record of when a password was created or changed.

- **Reset passwords.**

When resetting passwords, user identity must be verified. This can be done either in person or having the user answer questions for which the answers are only expected to be known by the user (i.e., not publicly available or easily attainable) that can be compared to the correct answers in the administrator's database. Passwords forgotten by their owner should be changed, not reissued.

Changing/Refreshing Passwords:

Users must be authenticated before resetting or distributing a password. Self-service password resets are commonly available in web based applications and identity management software. The function allows users who have forgotten passwords or inadvertently locked out their account to repair/reset it themselves without involvement of the help desk. The feature expedites problem resolution involving password resets but can also introduce in new attack vectors that could result in system compromise if implemented insecurely.

GSA does not encourage the use of knowledge-based questions in self-service password reset functions. The use of such functions must adhere to the guidance in NIST SP 800-63A regarding the use of knowledge-based verification of identity.

Password Storage:

All passwords must be encrypted in storage. Passwords must not be stored in forms (i.e., Windows dialog boxes, web forms, etc.). Do not store passwords in clear text form (unencrypted). Password-only mechanisms, especially those that transmit the password in the clear can be monitored and captured. Encryption converts data into unintelligible code. This process causes data to be unreadable to anyone who does not have the key to decrypt it. The data will remain private and confidential, regardless of whether it is being transmitted or stored on a computer when encrypted. Those without authorization will be unable to decrypt the encrypted passwords.

When a password is typed, the IT resource must determine whether it is right. If the IT resource stores the passwords unencrypted, anyone with access to the IT resource storage or backup tapes can steal passwords. It is not necessary for the IT resource to know a password to verify if it is correct.

Additional Contractor System Considerations: *Vendor/contractor systems must comply with the control IAW the guidance above and the AO must approve contractor recommended parameters.*

3.6 IA-6: Authenticator Feedback

Control: The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

GSA Implementation Guidance: Control IA-6 is applicable at all FIPS 199 levels.

The focus of this control is to assure that passwords which are entered into information systems are not visually displayed in clear text during entry. Typically, authenticator feedback is obscured by displaying asterisks instead of the actual password. The control does not cover feedback regarding the success or failure of an authentication attempt (which is covered by SI-11); and does not cover machine to machine authentication (which is addressed in IA-5).

Additional Contractor System Considerations: *Vendor/contractor systems must comply with the control IAW the guidance above.*

3.7 IA-7: Cryptographic Module Authentication

Control: The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

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

The focus of this control is to implement FIPS 140-2 certified encryption modules for authentication where encryption is required.

Requirements for encryption are determined via a Digital Identity Acceptance Statement and the FIPS 199 security categorization of the system (see control IA-2 for details). CIO 2100.1 states “*Web sites (internal and public) with logon functions, must implement TLS encryption with a FIPS 140-2 validated encryption module. SSL/TLS implementation must be IAW CIO-IT Security-14-69: SSL/TLS Implementation.*” Validated FIPS 140-2 Cryptographic Modules can be found by using the Advanced Search Type function on NIST’s Cryptographic Module Validation Program and selecting “140-2” as the Standard and “Active” as the Validation Status at the following URL.

<https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search>

Additional Contractor System Considerations: *Vendor/contractor systems must comply with the control IAW the guidance above.*

3.8 IA-8 Identification and Authentication (Non-Organizational Users)

Control: The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).

Control Enhancements:

- (1) Identification and Authentication (Non-Organizational Users) | Acceptance of PIV Credentials From Other Agencies. The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies;
- (2) Identification and Authentication (Non-Organizational Users) | Acceptance of Third-Party Credentials. The information system accepts only FICAM-approved third party credentials;
- (3) Identification and Authentication (Non-Organizational Users) | Use of FICAM-Approved Products. The organization employs only FICAM-approved information system components in [*all GSA information systems*] to accept third-party credentials;
- (4) Identification and Authentication (Non-Organizational Users) | Use Of FICAM-Issued Profiles. The information system conforms to FICAM-issued profiles.

GSA Implementation Guidance: Control IA-8 and enhancements (1), (2), (3), and (4) are applicable at all FIPS 199 levels.

In accordance with the Digital Identity Acceptance Statement, authentication of non-organizational users accessing federal information systems may be required to protect federal, proprietary, or privacy related information. Accordingly, a risk assessment is used in determining the authentication needs of the organization. Scalability, practicality, and security are simultaneously considered in balancing the need to ensure ease of use for access to federal information and information systems with the need to protect and adequately mitigate risk to organizational operations, organizational assets, individuals, other organizations. I&A requirements for information system access by organizational users are described in IA-2.

Additional Contractor System Considerations: *Vendor/contractor systems must comply with the control IAW the guidance above.*

4 Identification and Authentication and Supply Chain Risk Management

NIST SP 800-161 recommends Information and Communication Technology (ICT) Supply Chain Risk Management (SCRM) practices be used for FIPS 199 High systems. ICT SCRM processes increase the costs, both financial and time expended in supporting them, not just for GSA, but also for system integrators, suppliers, and service providers. ICT SCRM should be considered in the context of the system's missions, operational environments, and risks. Due to the increased costs involved in incorporating SCRM in IA processes the System Owner, IST Division Director, ISSM, and ISSO must carefully consider these costs prior to incorporating system specific SCRM processes involving IA. Any questions regarding SCRM should be sent to ispcompliance@gsa.gov.

NIST SP 800-161 states that it expands the *“identification and authentication control family to include identification and authentication of components, in addition to individuals (users) and processes acting on behalf of individuals within the ICT supply chain infrastructure. Identification and authentication is critical for ICT SCRM because it provides traceability of individuals, processes acting on behalf of individuals, and specific systems/components in an organization's ICT supply chain infrastructure. Identification and authentication is required to appropriately manage ICT supply chain risks to both reduce risks of ICT supply chain compromise and to help have needed evidence in case of ICT supply chain compromise.”*

The IA controls addressed in NIST SP 800-161, limited to those controls for FIPS 199 High systems, are provided in the following sections along with NIST SP 800-161 supplemental guidance on the controls and GSA's implementation guidance.

4.1 IA-1 Identification and Authentication Policy and Procedures (ICT SCRM)

NIST SP 800-161 Supplemental ICT SCRM Guidance: The organization should enhance their identity and access management policies to ensure that critical roles within the ICT supply chain infrastructure are defined and that the organization's critical systems, components, and processes are identified for traceability. This should include the identity of critical components that may not have been considered under identification and authentication in the past. Note that providing identification for all items within the supply chain would be cost-prohibitive and discretion should be used.

GSA Implementation Guidance: FIPS 199 High systems that have incorporated SCRM must adequately address identification and authentication risks associated with the ICT supply chain infrastructure. Protection commensurate with these risks must be implemented. For example, contract clauses may be used to require the identification and authentication of specific users or components in high value assets, especially when those users or components leave GSA or a GSA vendor's control.

Additional Contractor System Considerations: *No additional considerations, however vendor/contractor systems must comply with the control IAW the guidance above.*

4.2 IA-2 Identification and Authentication (Organizational Users) (ICT SCRM)

NIST SP 800-161 Supplemental ICT SCRM Guidance: Organizations should ensure that identification and authentication is defined for organizational users accessing the information system or ICT supply chain infrastructure. An organizational user may include employees as well as individuals deemed to have the equivalent status of employees (e.g., contractors, guest researchers, etc.) and may include system integrators fulfilling contractor roles. Criteria such as “duration in role” can aid in defining which identification and authentication mechanisms are used. The organization may choose to define a set of roles and associate a level of authorization to ensure proper implementation.

GSA Implementation Guidance: FIPS 199 High systems that have incorporated SCRM must adequately address I&A risks for organizational users associated with the ICT supply chain. The I&A requirements established for IA-2 apply when organizational users access the system’s supply chain infrastructure.

Additional Contractor System Considerations: *No additional considerations, however vendor/contractor systems must comply with the control IAW the guidance above.*

4.3 IA-4 Identifier Management (ICT SCRM)

NIST SP 800-161 Supplemental ICT SCRM Guidance: Identifiers allow for greater traceability. Within the organization's supply chain infrastructure, identifiers should be assigned to systems, individuals, documentation, devices, and components. In some cases, identifiers may be maintained throughout a system's life cycle, from concept to retirement, but at a minimum throughout the system's life within the organization. For software development, identifiers should be assigned for those components that have achieved configuration item recognition. For devices and operational systems, identifiers should be assigned when the items enter the organization’s ICT supply chain infrastructure, such as when they are transferred to the organization’s ownership or control through shipping and receiving or via download.

System integrators, suppliers, and external service providers typically use their own identifiers for tracking within their own ICT supply chain infrastructures. Organizations should correlate those identifiers with the organization-assigned identifiers for traceability and accountability. NIST SP 800-53 Revision 4 control IA-3 enhancements (4) and (5) are mechanisms that can be used to manage identities.

GSA Implementation Guidance: FIPS 199 High systems that have incorporated SCRM must adequately address identifier management risks associated with the ICT supply chain. The requirements established in IA-4 apply for identifier management throughout a system’s life within GSA.

Additional Contractor System Considerations: *No additional considerations, however vendor/contractor systems must comply with the control IAW the guidance above.*

4.4 IA-5 Authenticator Management (ICT SCRM)

NIST SP 800-161 Supplemental ICT SCRM Guidance: This control facilitates traceability and non-repudiation throughout the ICT supply chain infrastructure.

GSA Implementation Guidance: FIPS 199 High systems that have incorporated SCRM must adequately address authenticator management risks associated with the ICT supply chain. The requirements established in IA-5 apply when addressing the management of authenticators in the supply chain.

Additional Contractor System Considerations: *No additional considerations, however vendor/contractor systems must comply with the control IAW the guidance above.*

4.5 IA-8 Identification and Authentication (Non-Organizational Users) (ICT SCRM)

NIST SP 800-161 Supplemental ICT SCRM Guidance: System integrators, external services providers, and suppliers have the potential to engage the organization's ICT supply chain infrastructure for service delivery (development/integration services, product support, etc.). Organizations should manage the establishment, auditing, use, and revocation of identification and authentication of non-organizational users within the ICT supply chain infrastructure. Organizations should ensure promptness in performing identification and authentication activities, especially in the case of revocation management, to help mitigate against ICT supply chain risks such as insider threat.

GSA Implementation Guidance: FIPS 199 High systems that have incorporated SCRM must adequately address I&A risks for non-organizational users associated with the ICT supply chain. The requirements established for IA-8 apply when non-organizational users access the system or supply chain.

Additional Contractor System Considerations: *No additional considerations, however vendor/contractor systems must comply with the control IAW the guidance above.*

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.

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.

Adequate Security

Security commensurate with the risk resulting from the loss, misuse, or unauthorized access to or modification of information.

Assurance

Grounds for confidence that the other four security goals (integrity, availability, confidentiality, and accountability) have been adequately met by a specific implementation. "Adequately met" includes (1) functionality that performs correctly, (2) sufficient protection against unintentional errors (by users or software), and (3) sufficient resistance to intentional penetration or by-pass.

Authentication

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

Authenticator

The means used to confirm the identity of a user, processor, or device (e.g., user password or token).

Authenticity

The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. See Authentication.

Authorization

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

Confidentiality

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

Encryption

Conversion of plaintext to ciphertext through the use of a cryptographic algorithm.

Identity

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

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.

Identifier

Unique data used to represent a person's identity and associated attributes. A name or a card number are examples of identifier.

Integrity

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

Multifactor Authentication (MFA)

Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g., password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric).

Network

Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

Network Access

Access to an organizational information system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, Internet).

Organization

A federal agency, or, as appropriate, any of its operational elements.

Organizational User

An organizational employee or an individual the organization deems to have equivalent status of an employee (e.g., contractor, guest researcher, individual detailed from another organization, individual from allied nation).

Password

A secret that a Claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings

Privileged Account

An information system account with approved authorizations of a privileged user.

Privileged User

A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

Remote Access

Access to an organizational information system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the Internet).

Security Control Enhancements

Statements of security capability to 1) build in additional, but related, functionality to a basic control; and/or 2) increase the strength of a basic control.

Validation

The process of demonstrating that the system under consideration meets in all respects the specification of that system;

Verification

Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled (e.g., an entity's requirements have been correctly defined, or an entity's attributes have been correctly presented; or a procedure or function performs as intended and leads to the expected outcome).