EPA INFORMATION PROCEDURES

OFFICE OF ENVIRONMENTAL INFORMATION

| | | | |
|---|---|---|---|
| EPA Classification No.: | CIO-2150.3-P-07.1 | CIO Approval Date: | 08/06/2012 |
| CIO Transmittal No.: | 12-003 | Review Date: | 08/06/2015 |

*Issued by the EPA Chief Information Officer,*
*Pursuant to Delegation 1-19, dated 07/07/2005*

# INFORMATION SECURITY –
# INTERIM IDENTIFICATION AND AUTHENTICATION PROCEDURE
# V2.1
# JULY 13, 2012

## 1. PURPOSE

The purpose of this procedure is to facilitate the implementation of Environmental Protection Agency (EPA) security control requirements for the Identification and Authentication control family, as identified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 3 *Recommended Security Controls for Federal Information Systems and Organizations*.

## 2. SCOPE AND APPLICABILITY

These procedures cover all EPA information and information systems to include those used, managed, or operated by a contractor, another agency, or other organization on behalf of the Agency.

These procedures apply to all EPA employees, contractors, and all other users of EPA information and information systems that support the operations and assets of EPA.

## 3. AUDIENCE

These procedures apply to all EPA employees, contractors, and all other users of EPA information and information systems that support the operations and assets of EPA.

## 4. BACKGROUND

Based on federal requirements and mandates, the EPA is responsible for ensuring that all offices within the Agency meet the minimum security requirements defined in the Federal Information Processing Standards (FIPS) Publication 200, Minimum Security Requirements for Federal Information and Information Systems. All EPA information systems must meet the security requirements through the use of the security controls defined in the NIST SP 800-53, Revision 3 *Recommended Security Controls for Federal Information Systems and Organizations*. This chapter addresses the procedures and standards set forth by EPA, and in compliance with, the identification and authentication family of controls found in NIST SP 800-53, Revision 3.

## 5. AUTHORITY

- E-Government Act of 2002, Public Law 107-347, Title III*, Federal Information Security Management Act (FISMA)* as amended
- Freedom of Information Act (FOIA), 5 U.S.C. § 552, as amended by Public Law No.

104-231, 110 Stat. 3048, Electronic Freedom of Information Act Amendments of 1996

- Clinger-Cohen Act of 1996, Public Law 104-106
- Paperwork Reduction Act (44 USC 3501-3519) May 1995
- Privacy Act of 1974 (5 USC § 552a), as amended
- USA PATRIOT Act (P.L. 107-56), October 2001
- Code of Federal Regulations, Part 5 Administrative Personnel, Subpart C—*Employees Responsible for the Management or Use of Federal Computer Systems*, Section 930.301 through 930.305 (5 C.F.R 930.301-305)
- Office of Management and Budget (OMB) Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies,* December 2003
- OMB Memorandum M-05-24, Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*, August 2004
- OMB Memorandum M-06-16, "*Protection of Sensitive Agency Information*," June 2006
- OMB Memorandum M-07-11, "*Implementation of Commonly Accepted Security Configurations for Windows Operating Systems*," March 2007
- OMB Memorandum M-08-05, "*Implementation of Trusted Internet Connections (TIC)*," November 2007
- OMB Memorandum M-08-22, "*Guidance on the Federal Desktop Core Configuration (FDCC)*," August 2008
- Federal Information Processing Standards (FIPS) 140-2, *Security Requirements for Cryptographic Modules*, May 2001
- FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004
- FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006
- FIPS 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, March 2006
- EPA Information Security Program Plan
- EPA Information Security Policy

## 6. PROCEDURES

### IA-2 – Identification and Authentication (Organizational Users)

a. The information system must be configured to uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users).

*Note: Organizational users include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors, guest researchers, individuals from allied nations).*

i. Users must be uniquely identified and authenticated for all access other than those accesses explicitly identified and documented as exceptions regarding permitted actions without identification and authentication.

- Refer to *Information Security – Interim Access Control Procedures* for requirements on permitted actions without identification and authentication.

ii. Unique identification of individuals in group accounts (e.g., shared privilege accounts) may need to be considered for detailed accountability of activity.

b. In addition to identifying and authenticating users at the information system level (i.e., at log-on), identification and authentication mechanisms must be employed at the application level, when necessary, to provide increased security for the information system and the information it processes.

c. Authentication of user identities must be accomplished through the use of passwords, Personal Identification Numbers (PINs), tokens, biometrics, or in the case of multifactor authentication, some combination thereof.

d. An Electronic Authentication ("E-Authentication") Risk Assessment must be conducted for any Agency information system that requires authentication over the Internet.

i. This E-Authentication Risk Assessment (ERA) must be conducted in accordance with OMB M-04-04 or its successors and must be used to determine the compliance requirements for access consistent with FIPS 190, as amended.

ii. The ERA may be conducted as part of conducting a general risk assessment under EPA Risk Assessment Procedures or it may be a separate activity, in which case it must be informed by a general risk assessment for the information system.

- Refer to *Information Security – Interim Risk Assessment Procedures* for requirements on conducting a risk assessment.

iii. The ERA process must identify potential impacts should proper authentication fail or should there be an authentication error.

- These impacts are rated as low, moderate, or high risks.

iv. The identified risks must then be mapped to the appropriate assurance level. OMB M-04-04 sets four identity authentication assurance levels:

- Level 1: Little or no confidence in the asserted identity's validity.
- Level 2: Some confidence in the asserted identity's validity.
- Level 3: High confidence in the asserted identity's validity.
- Level 4: Very high confidence in the asserted identity's validity.

v. The information system's System Security Plan (SSP) must state if E-Authentication is required, and, if not required, an explanation must be included.

vi. Technologies for E-Authentication must then be selected and implemented based on technical guidance provided in NIST SP 800-63, as amended.

- Authenticators (e.g., passwords, randomly generated PINs, tokens, biometric, and other authenticators) and the selected technologies must comply with Level 2, 3, or 4 requirements.
- Technology selection must be based first on technology standards or approved technologies within EPA's approved technology and security architecture.
- If available technologies and mechanisms prove inadequate, alternatives that are consistent with NIST guidance may be proposed.

vii. The guidance provided by NIST SP 800-63, must apply to both local and remote access to the information system.

- Remote access connections must be both authenticated and authorized to be accepted.

viii. Validation must be conducted to ensure that the implemented system has met the required assurance level.

ix. Subsequent to the ERA and in accordance with requirements of the information system's life cycle stage and Certification and Accreditation (C&A) Security Authorization requirements, the information system must be periodically reassessed to determine technology refresh requirements.

e. FIPS 201-1 and NIST SP 800-73, 800-76, and 800-78 must be used as guidance on Personal Identify Verification (PIV) credentials for use in the unique identification and authentication of federal employees and contractors.

**For moderate and high information systems**

f. The information system must use multifactor authentication for network access to non-privileged accounts.

g. The information system must use multifactor authentication for local access to privileged accounts.

h. The information system must use multifactor authentication for network access to privileged accounts.

i. The information system must use replay-resistant authentication protocols for network access to privileged accounts.

*Note: An authentication process resists replay attacks if it is impractical to achieve a successful authentication by recording and replaying a previous authentication message. Techniques used to address this include protocols that use challenges (e.g., Transport Layer Security TLS), and time synchronous or challenge-response one-time authenticators.*

**IA-3 – Device Identification and Authentication**

**For moderate and high information systems**

a. The information system must be configured to uniquely identify and authenticate end user-operated devices (e.g. workstations, laptops, Voice over Internet Protocol (VoIP) phones, cell phones) and servers before establishing a connection.

b. The required strength of the device authentication mechanism must be determined by the security categorization of the information system as well as an assessment of risk incurred.

c. Host or device authentication must use only approved procedures, mechanisms, or protocols.

i. Approved mechanisms and protocols include, but are not limited to, the following:

- Media Access Control (MAC) address filtering, which provides basic filtering based on Open Systems Interconnection (OSI) Layer 2 (Data Link Layer) address information. This control is appropriate for implementation within information systems categorized as low on a wired network for *limited-use devices*, or *devices with limited functionality*, such as VoIP phones.
- Vendor-specific solutions such as Cisco's Port Security, which provide basic identification and authentication for devices in a wired network on a per-port basis. This control is appropriate for implementation on a wired network in an information system categorized low or moderate.
- Wi-Fi Protected Access 2 (WPA2) in combination with MAC filtering. This control is appropriate for implementation on a wireless network in an information system categorized as low or moderate.
- Institute of Electrical and Electronics Engineers (IEEE) 802.1x. This control

is appropriate for implementation on a wired or wireless network in an information system categorized as low, moderate, or high. Network Access Control (NAC) technology, which is most commonly built on the foundations of 802.1x, is the preferred method for device identification and authentication within EPA information systems.

d. The procedures, mechanisms, or protocols used for device identification and authentication must be clearly documented, with diagrams, in the SSP.

**IA-4 – Identifier Management**

a. Information system identifiers for users and devices must be selected such that the identifier uniquely identifies an individual or device.
   i. Assignment of user identifiers must ensure that no two users have the same identifier, to ensure user accountability.
   ii. A User Principal Name (UPN) must be implemented for each EPA issued smart card consisting of a unique user name and in accordance with EPA's e-mail standard naming convention or Internet Request for Comment (RFC) 2822, April 1 2001, as appropriate.
      - Systems that do not implement smart card access must use a unique UPN username as an identifier.
   iii. User names must support the ready identification of employees and contractor employees (e.g., doe, john).
b. Authorization must be received from a designated organizational official to assign a user or device identifier.
   i. An EPA sponsor shall issue user identifiers.
c. The user identifier must be assigned only to the intended party.
d. The device identifier must be assigned only to the intended device.
e. Inactive user identifiers must be:
   i. Automatically disabled after 30 days of inactivity unless otherwise authorized by a supervisor.
   ii. Users can be allowed to self-activate disabled accounts within 180 after the account has been automatically disabled.
f. User and device identifiers must not be reused for up to three years after the account has been deleted.
   i. Longer periods may be specified as required for records retention purposes.
g. Default user names such as "sysadmin" or "administrator" must be changed *before* implementation of the information system or component (e.g. routers, switches, firewalls, printers, workstations, and servers).

**IA-5 – Authenticator Management**

a. The identity of the individual or device receiving an information system authenticator must be verified as part of the initial authenticator distribution.
b. Unique initial authenticator content must be established for user and device authenticators.

*Note: Initial authenticator content is the actual content (e.g., the initial password) as opposed to requirements about authenticator content (e.g., minimum password length).*

c. Authenticators for users and devices must have sufficient strength of mechanism for their intended use.

*Note: User authenticators include, for example, tokens, Public Key Infrastructure (PKI) certificates, biometrics, passwords, and key cards ("smart cards").*

d. Administrative procedures must be established and implemented for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators.
   i. If a user knows or suspects that their password has been compromised, they shall immediately:
      - Notify their supervisor.
      - Report a known or potential security breach to the EPA help desk.
      - Request the EPA help desk to reset or change their password or if self-service password mechanisms are used, immediately change their own password.

e. Default content of authenticators (i.e., passwords provided for initial entry to a system) must be changed *before* implementation of the information system or component (e.g. routers, switches, firewalls, printers, workstations, servers).
   i. The information system owner shall confirm that software and/or hardware upgrades, updates, and patches have not reinstalled default passwords.

f. Authenticators must be changed or replaced periodically.
   i. All newly assigned passwords must be changed the first time a user logs into the information system.
   ii. Passwords must be set to automatically expire in 90 days or sooner.
   iii. PIV (Smart Cards) certificates must be renewed every three (3) years.

g. The following minimum and maximum lifetime restrictions and re-use conditions must be adhered to regarding authenticators:
   i. Passwords must have a minimum lifetime of 1 days and a maximum lifetime of 90 days.
      - Unless authorized by the information system owner, passwords cannot be changed in less than one (1) day.
   ii. Password reuse is prohibited for 24 generations.
      - Password history must be set with a history of at least 24 passwords, so a user cannot quickly re-use a previous password.

h. Authenticator content must be protected from unauthorized disclosure and modification.

i. Users shall take reasonable and specific measures to safeguard authenticators.
   i. Users shall maintain possession of their individual authenticators, not loan or share authenticators with others, and report lost or compromised authenticators immediately to their supervisor and the EPA help desk as a security event.
   ii. Devices must be configured to safeguard authenticators (e.g., certificates, passwords).

j. For password-based and PIN based authentication, the information system must enforce the following:
   i. Passwords must be at least twelve characters long.
   ii. The PIN must be eight numerical digits at a minimum.
   iii. All passwords, including initial passwords must be composed of characters from

each of the following four categories, as provided in the application or operating system schema:

- Uppercase letters (e.g., A, B, C, Y, Z, etc.)
- Lowercase letters (e.g., a, b, c, y, z, etc.)
- Special characters (e.g., ! @, #, $, %, ^, &, etc.)
- Numbers (e.g., 1, 2, 3, 4, 5, etc.)

iv. Passwords must not contain any of the following:

- Dictionary words (e.g., computer, work) or common names (e.g., Betty, Fred, Rover).
- Portions of associated account names (e.g., user ID, login name).
- Consecutive character strings (e.g., abcdef, 12345).
- Simple keyboard patterns (e.g., QWERTY, asdfgh).
- Generic passwords (i.e., password consisting of a variation of the word “password” [e.g., P@ssw0rd1]).

v. At least 50% of total password content must be changed when a new password is created.

vi. Prohibit passwords and PINs from being displayed when entered.

vii. Encrypt passwords and PINs when stored and transmitted.

k. A waiver of the password requirements and standards may be requested, provided the request includes at a minimum:

   i. Specific designation of which requirement(s) the waiver request is addressing.

   ii. A detailed analysis of the password resistance to compromise in accordance with password entropy and strength factors detailed in Appendix A of NIST SP 800-63, as amended.

l. FIPS 201-1 and NIST SP 800-73, 800-76, and 800-78 must be used as guidance on PIV credentials.

m. NIST SP 800-63 must be used as guidance on remote electronic authentication.

**For moderate and high information systems**

n. For PKI-based authentication, the information system must enforce the following:

   i. Validate certificates by constructing a certification path with status information (e.g., certificate revocation lists, online certificate status protocol responses) to an accepted trust anchor.

   ii. Enforce authorized access to the corresponding private key.

   iii. Map the authenticated identity to the user account.

o. The registration process to receive one-time token generators, such as RSA SecureID and/or PIV Cards must be carried out in person before a designated registration authority with authorization by a designated organizational official.

p. The registration process to receive an account with privileged access to the information system must be carried out in person before a designated registration authority with an authorization by a designated organizational official.

q. NIST SP 800-25 must be used as guidance on PKI technology.

### IA-6 – Authenticator Feedback

a. The information system must obscure feedback of authentication information during the authentication process to protect the information from possible exploitation or use by unauthorized individuals.

   i. Passwords must be masked upon entry (e.g., displaying asterisks or dots when a user types in a password) and not displayed in clear text.

b. The feedback from the information system must not provide information that would allow an unauthorized user to compromise the authentication mechanism.

**IA-7 – Cryptographic Module Authentication**

a. The information system must use 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.

   i. Access via the Internet by authenticated personnel to authorized EPA data communications network-attached resources must be encrypted as established for the federal government by FIPS 140-2 using an Office of Technology Operations and Planning (OTOP)-approved technique.

   ii. Additional information on the process of validating the cryptography algorithm implementation and validation of Cryptographic modules can be found at http://csrc.nist.gov/groups/STM/index.html http://csrc.nist.gov/groups/STM/cmvp/validation.html and http://csrc.nist.gov/cryptval

**IA-8 – Identification and Authentication (Non-Organizational Users)**

a. The information system must be configured to uniquely identify and authenticate non-organizational users (or processes acting on behalf of non-organizational users).

*Note: Non-organizational users include all information system users other than organizational users explicitly covered by IA-2.*

   i. Non-organizational users must be uniquely identified and authenticated for all access other than those accesses explicitly identified and documented as exceptions regarding permitted actions without identification and authentication.

      - Refer to *Information Security – Interim Access Control Procedures* for requirements on permitted actions without identification and authentication.

b. A risk assessment must be used to determine the authentication needs of the organization.

   i. In accordance with the E-Authentication E-Government initiative, authentication of non-organizational users accessing federal information systems may be required to protect federal, proprietary, or privacy-related information (with exceptions noted for national security systems).

   ii. Scalability, practicality, and security should be 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 EPA's operations, EPA's assets, individuals, other organizations, and the Nation.

c. Refer to IA-2 for identification and authentication requirements regarding information system access by organizational users.

## 7. RELATED DOCUMENTS

- NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook, October 1995
- NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996
- NIST SP 800-25, *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*, October 2000
- NIST SP 800-36, Guide to Selecting Information Technology Security Products, October 2003
- NIST SP 800-41, Revision 1, Guidelines on Firewalls and Firewall Policy, September 2009
- NIST SP 800-43, Systems Administration Guidance for Windows 2000 Professional, November 2002
- NIST SP 800-44, Version 2, Guidelines on Securing Public Web Servers, September 2007
- NIST SP 800-45, Version 2, Guidelines on Electronic Mail Security, February 2007
- NIST SP 800-46, Revision 1, Guide to Enterprise Telework and Remote Access Security, June 2009
- NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations, August 2009*
- NIST SP 800-63, Version 1.0.2, *Electronic Authentication Guide,* April 2006
- NIST SP 800-68 Revision 1, Guidance for Securing Microsoft Windows XP Systems for IT Professionals, October 2008
- NIST SP 800-69, Guidance for Securing Microsoft Windows XP Home Edition, September 2006
- NIST SP 800-73-3, *Interfaces for Personal Identity Verification*, February 2010
- NIST SP 800-76-1, *Biometric Data Specification for Personal Identity Verification*, January 2007
- NIST SP 800-78-2, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, February 2010
- NIST SP 800-81, Secure Domain Name System (DNS) Deployment Guide, May 2006
- NIST SP 800-87, Revision 1, Codes for Identification of Federal and Federally-Assisted Organizations, April 2008
- NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS), February 2007
- NIST SP 800-95, Guide to Secure Web Services, August 2007
- NIST SP 800-96, PIV Card to Reader Interoperability Guidelines, September 2006
- NIST SP 800-104, A Scheme for PIV Visual Card Topography, June 2007
- NIST SP 800-113, Guide to SSL VPNs, July 2008
- NIST SP 800-116, A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS), November 2008
- NIST SP 800-123, Guide to General Server Security, July 2008
- NIST SP 800-124, *Guidelines on Cell Phone and PDA Security*, October 2008
- RFC2822: *Internet Message Format*, April 2001

## 8. ROLES AND RESPONSIBILITIES

**Office of Technology Operations and Planning (OTOP), Office of Environmental Information (OEI)**

a. OEI, OTOP has the following responsibilities with respect to identification and authentication:
   i. Provide central management of identification and authentication to ensure unique naming of users and devices.
   ii. Develop enterprise identification and authentication standards as needed to ensure consistency.
   iii. Coordinate with the Office of Administration and Resources Management (OARM) on personnel and identification requirements associated with smart card issuance and implementation.

**Office of Administration and Resources Management (OARM)**

a. OARM has the following responsibilities with respect to identification and authentication:
   i. Coordinate with OEI on personnel and identification requirements associated with smart card issuance and implementation.
   ii. Ensure that smart card certificates are compatible and capable of implementing identification and authentication requirements.

**Information System Owner (SO)**

a. The ISO has the following responsibilities with respect to identification and authentication:
   i. Conduct an ERA.
   ii. Manage user and device identifiers, as applicable.
   iii. Ensure that upgrades or patches have not reinstalled factory default passwords or other types of backdoors.
   iv. Ensure that appropriate identification, authentication, and authorization are implemented.

**Information Security Officers**

a. ISOs have the following responsibilities with respect to identification and authentication:
   i. Provide day-to-day management of identification and authentication for the information system including, but not limited to:
      - Configuration of the requirements.
      - Periodic monitoring of the requirements.

**Users/Individuals**

a. Users/individuals have the following responsibilities with respect to identification and authentication:
   i. Immediately notify their supervisors if they suspect their password or PIN or other authenticator has been compromised.
   ii. Report a known or potential security breach to the EPA help desk.
   iii. Immediate change a compromised password or request the EPA help desk to reset or change their password.
   iv. Take reasonable measures to safeguard authenticators.

## 9. DEFINITIONS

- Assurance – for identity authentication, (1) the degree of confidence in the vetting process used to establish the identity of the individual to whom the credential was issued, and (2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.
- Authentication - the process of verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
- Identity - a unique name of an individual person. Since the legal names of persons are not necessarily unique, the identity of a person must include sufficient additional information (for example an address, or some unique identifier such as an employee or account number) to make the complete name unique.
- Local Access – 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.
- Multifactor Authentication – the process of using two or more different factors for verifying identity. Factors usually typically categorized as “something you know” (e.g., a password), “something you have” (e.g., a token), and “something you are” (e.g., a biometric).
- Network Access – 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.
- Non-Organizational Users – all information system users other than organizational users explicitly covered by IA-2.
- Organizational Users – organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors, guest researchers, individuals from allied nations).
- Remote Access – a type of network access which involves communication through an external network (e.g., the Internet).
- Signature (of an individual) – a mark or sign made by an individual to signify knowledge, approval, acceptance, or obligation. Can be accomplished manually, sometimes referred to as a “wet signature,” or electronically.
- Written – or “in writing” means to officially document the action or decision and includes a signature. The documentation can be accomplished manually or electronically.

## 10. WAIVERS

Waivers may be requested from the CIO by submitting a justification based on:

- substantive business case need(s)
- demonstration of, or a proposal for, establishment of adequate compensating controls that provide a suitable alternative to the mandated protection

The CIO may grant a waiver for sufficient reasons exercising judgment in the best interests of the Agency.

The SAISO and Director, OTOP shall coordinate to maintain central repository of all waivers.

## 11. RELATED POLICY, PROCEDURES, STANDARDS AND GUIDELINES

Related policy and procedures are available on OEI's Policy Resources website.

**http://intranet.epa.gov/oei/imitpolicy/policies.htm**

Related standards and guidelines are available on OEI's website.

## 12. MATERIAL SUPERSEDED

*EPA Information Security Manual, Directive 2195A1*, 1999 Edition, Sections 7.2 (in part), 11.1, and 11.2.6

## 13. ADDITIONAL INFORMATION

NA

***Malcolm D. Jackson***
***Assistant Administrator and Chief Information Officer***
***Office of Environmental Information***

## APPENDIX A: ACRONYMS

| | |
|---|---|
| C&A | Certification and Accreditation |
| EPA | Environmental Protection Agency |
| ERA | Electronic Authentication Risk Assessment |
| FIPS | Federal Information Processing Standards |
| FISMA | Federal Information Security Management Act |
| IT | Information Technology |
| MAC | Media Access Control |
| NIST | National Institute of Standards and Technology |
| OARM | Office of Administration and Resources Management |
| OEI | Office of Environmental Information |
| OMB | Office of Management and Budget |
| OTOP | Office of Technology Operations and Planning |
| PIN | Personal Identification Number |
| PIV | Personal Identity Verification |
| PKI | Public Key Infrastructure |
| P.L. | Public Law |
| RFC | Request for Comment |
| SSP | System Security Plan |
| SP | Special Publication |
| TLS | Transport Layer Security |
| UPN | User Principal Name |
| USC | United States Code |

## DOCUMENT CHANGE HISTORY

| Version | Release Date | Summary of Changes | Author of Changes | DCN |
|---|---|---|---|---|
| 0.6 | 1/22/09 | Initial draft | Heather Flager | Procedures-IA-Draft_TO62_020_1 |
| 1.0 | 6/26/09 | Incorporated EPA comments<br>Final | Heather Flager | Procedures-IA-Final_TO62_020_2 |
| 1.8 | 6/21/10 | Updated per NIST SP 800-53 Rev 3 | Heather Flager | Procedures_IA_Draft.TO-062_050_1.0 |
| 1.8 | 7/14/2010 | TISS comments/changes | Charleen Johnson | Procedures_IA_Draft.TO-062_050_1.0 |
| 1.9 | 12/27/2010 | TISS Final Draft Review | Charleen Johnson | Procedures_IA_Draft.TO-062_050_1.0 |
| 2.0 | 5/2/2012 | SAISO Final Review | Abe Getchell | Procedures_IA_Draft.TO-062_050_1.0 |
| 2.1 | 7/13/12 | Document Review | LaToya Gordon | Procedures_IA_Draft.TO-062_050_1.0 |