EPA Classification No.:	CIO-2150.3-P-13.1	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 PERSONNEL SECURITY PROCEDURES
V2.0
JULY 18, 2012

1. PURPOSE

The purpose of this procedure is to facilitate the implementation of Environmental Protection Agency (EPA) security control requirements for the Personnel Security 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 operation 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 personnel security 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 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 of 1995 (44 USC 3501-3519)
- Privacy Act of 1974 (5 USC § 552a) as amended
- USA PATRIOT Act of 2001, Public Law 107-56
- 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)
- Title 5 Code of Federal Regulations (C.F.R.), Chapter 1 - Office of Personnel Management (OPM), Subchapter B – Civil Service Regulations, Part 731 – Suitability
- Executive Order 10450 (as amended), *Security Requirements for Government Employment*, April 1953
- Executive Order 12968, *Access to Classified Information*, August 1995
- Office of Management and Budget (OMB) Circular A-130, "*Management of Federal Information Resources*", Appendix III, "*Security of Federal Automated Information Resources*", November 2000
- Federal Information Processing Standards (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

PS- 2 – Position Categorization

a. A risk designation must be assigned to all competitive service information management and information technology related positions.

   i. Screening criteria must be established for individuals filling those positions in accordance with *Security Requirements for Government Employment* (Executive Order 10450), OPM policy and guidance, and *EPA's Risk Designation Fact Sheet*.

   ii. Screening criteria must include explicit information security role appointment requirements (e.g., training, security clearance).

b. A risk designation must be assigned to all non-federal position functions (as determined according to the equivalent of a federal employee in the same function) in information management and information technology related positions.

   i. Screening criteria must be established for individuals filling those positions in accordance with requirements of federal employees.

c. The risk designation process must comply with the requirements in the *Personnel Security Handbook*.

d. The following must be considered with respect to position risk designations:

   i. Program-level risk must be factored into the position risk designation.

   ii. The risk level associated with each user role that has access to the information system must be assessed.

   iii. A position's risk designation must consider:

   - Physical access to the information system's hardware or software.
   - The ability to override or bypass security controls.
   - The scope of IT resources potentially impacted by security violations.
   - The FIPS 199 security categorization of the information system.

e. Position risk designations must be reviewed and revised according to the following criteria:

   i. At a minimum, every three (3) years when completed in conjunction with the appraisal process.

   ii. When a change to or addition of duties occurs.

f. Components shall designate the position sensitivity level for all Government and contractor positions that use, develop, operate, or maintain information systems and shall determine risk levels for each contractor position. Position sensitivity levels shall be reviewed annually and revised as appropriate.

<u>PS- 3– Personnel Screening</u>

a. Individuals must undergo background screening prior to being authorized access to the information system.

b. Individuals must be rescreened in accordance with FIPS 199; 200, EPA Order 3200 and Executive Order 10450 where conditions requiring rescreening, where rescreening is so indicated, and the frequency of such rescreening.

c. Personnel screening and rescreening must be consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidance, and the criteria established for the risk designation of the assigned position.

   i. Individuals must be rescreened in accordance with FIPS 199; 200, EPA Order 3200 and Executive Order 10450, i.e., every three (3) years in conjunction with Personal Identity Verification (PIV) re-issuance.

d. Components shall ensure the incumbents of these positions have favorably adjudicated background investigations commensurate with the defined position sensitivity levels.

Note: The organization may define different rescreening conditions and frequencies for personnel accessing the information system based on the type of information processed, stored, or transmitted by the system.

PS- 4– Personnel Termination

Note: Timely execution of this procedure is particularly essential for employees or contractors terminated for cause (i.e., involuntary termination).

a. The following actions must be taken upon the termination of an individual's employment:

   i. Conduct exit interviews.

      - Counsel the terminated individual on continued obligations under information system non-disclosure, confidentiality, or user access agreements.
      - Determine all information systems to which the individual had access and email distribution list memberships.

Note: Exit interviews ensure that individuals understand any security constraints imposed by being former employees and that proper accountability is achieved for all information system-related property. Exit interviews may not be possible for some employees (e.g., in the case of job abandonment, some illnesses, and nonavailability of supervisors). Exit interviews are important for individuals with security clearances.

   ii. Notify information system management of information system and facility access termination requirements.

   iii. If termination is voluntary (i.e., normal, scheduled), terminate information system access within the same day of notification of such termination (i.e., same day the individual is terminated).

      - Disable each password or lock each account.
      - Refer to *Information Security – Access Control Procedures* for requirements on information system access controls.

   iv. If termination is involuntary (i.e., emergency, adverse), terminate information system access within four (4) hours of notification of such termination (i.e., same day the employee is terminated).

      - Disable each password or lock each account.
      - Refer to *Information Security – Access Control Procedures* for requirements on information system access controls.

   v. Retrieve all security-related EPA information and system-related property (e.g., hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes).

   vi. Obtain access to EPA information and information systems formerly controlled by the terminated individual.

- Prior to archiving or permanent disabling of accounts, transfer all Agency information to appropriate personnel or archives.

b. In the event of an adverse removal or involuntary termination, rotate the employee or contractor to a non-sensitive position or restrict access or rights to information systems before notification, whenever possible, to avoid the potential for malicious actions to information systems.

c. The following activities must be performed for all personnel, including contractors, leaving, changing jobs, or on extended absences:

   i. Change or cancel all passwords, codes, user IDs, and locks.

   ii. Disable user IDs for extended absences (60 days).

   iii. Update access control lists, mailing lists, etc.

   iv. Collect all keys, badges, and similar items.

   v. Reconcile any financial accounts over which the employee had control.

   vi. Ensure electronic records are accessible and properly secured, filed, or appropriately disposed.

d. Individuals who have been suspended or terminated and have had their access removed must repeat authorization procedures in order to receive official access again.

e. The Senior Information Official (SIO) shall certify that termination procedures have been complied with.

   i. The certifying statements must be kept on file for inspection by the Office of Environment Information (OEI) or the Office of Inspector General (OIG).

f. Access controls for information systems must be reviewed every 30 days to verify that the access lists have been updated regarding terminated individuals.

   i. Refer to *Information Security – Access Control Procedures* for requirements on access controls.

PS- 5– Personnel Transfer

Note: This control applies when the reassignment or transfer of an employee is permanent or of such an extended duration as to make the actions warranted.

a. Logical and physical access authorizations to information systems and facilities must be reviewed when personnel are reassigned or transferred to other positions within the Agency and the appropriate actions must be initiated.

   i. The actions undertaken must be driven by the individual's position risk designation.

   ii. Refer to the *Personnel Security Handbook* for requirements on personnel reassignments and transfers, whether permanent or temporary.

b. The following activities must be performed for all personnel, including contractors, upon personnel reassignment or transfer:

   i. Change or cancel all passwords, codes, and user IDs.

ii. Update access control lists, mailing lists, etc.

iii. Reconcile any financial accounts over which the employee had control.

iv. Ensure electronic records are accessible and properly secured, filed, or appropriately disposed.

v. Collect old keys, identification cards, authentication tokens, and building passes.

vi. Issue new keys, identification cards, authentication tokens, and building passes.

vii. Close previous information system accounts.

Note: A user's account may be kept and modified as appropriate as long as the individual, the original supervisor, and the new supervisor carefully review the account to ensure that no resources or access privileges are left on the account and the account has only the resources and privileges appropriate to the person's new role and responsibilities.

viii. Establish new accounts.

- The individual's access privileges and authorizations must be reviewed and updated to be in alignment with the new position on the effective date.

ix. Change information system and facility access authorizations.

- Individual information system and facility access authorizations must be reviewed and appropriately aligned or re-aligned with the new position's required accesses and authorizations.

x. Provide for access to official records to which the individual employee had access at the previous work location and in the previous information system accounts.

c. The transfer or reassignment actions must be initiated within 24 hours following the formal transfer action.

d. Reviews of logical and physical access authorization to the information systems and faciliities when personnel are reassigned or transferred to other positions within the organization and initiates within 24 hours.

e. The SIO shall certify that personnel transfer procedures have been complied with.

i. The certifying statements must be kept on file for inspection by the OEI or the OIG.

f. Access controls for information systems must be reviewed every 30 days to verify that the access lists have been updated regarding transferred individuals.

i. Refer to *Information Security – Access Control Procedures* for requirements on access controls.

PS- 6– Access Agreements

a. Appropriate access agreements (e.g., nondisclosure agreements, acceptable use agreements, rules of behavior, conflict-of-interest agreements) must be signed by individuals requiring access to Agency information and information systems prior to being granted access.

   i. Signed access agreements must include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with the information system to which access is authorized.

b. Access agreements must state that penalties for non-compliance may include sanctions and possible criminal and/or civil prosecution.

   i. Specific penalties as identified in the applicable law or U.S. Code must be included, as appropriate.

c. The access agreements must be reviewed and updated (i.e., redistributed and signatures collected) as follows:

   i. Annually.

   ii. Whenever there is a significant change to the information system or information being processed.

   iii. Whenever there is a change to the agreements' verbiage.

Note: Electronic signatures are acceptable for use in acknowledging access agreements unless specifically prohibited by Agency policy.

d. An individual's current, signed access agreements must be kept on file for one fiscal year after termination.

<u>PS- 7– Third-Party Personnel Security</u>

a. Personnel security requirements including security roles and responsibilities for third-party providers (e.g., service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, network and security management) must be established.

b. Personnel security requirements must be documented.

c. Personnel security requirements must be explicitly included in acquisition-related documents.

   i. Refer to *Information Security – System and Services Acquisition Procedures* for requirements on acquisitions.

d. The Contracts Officer and Contracting Officer Technical Representative (COTR) shall ensure that contractors and other third-party service providers are subject to the same personnel screening requirements as EPA personnel.

e. Provider compliance with personnel security requirements must be monitored.

f. NIST SP 800-35 must be used as guidance on information technology security services.

<u>PS- 8– Personnel Sanctions</u>

a. EPA shall employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.

i. Refer to *Information Security – Security Planning Procedures* for requirements on rules of behavior.

b. The sanctions process must be consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance where applicable.

i. The sanctions process must also address the following:

- Informal corrective actions.
- Formal disciplinary actions.
- Severe disciplinary actions.
- Removal of system access.
- Possible criminal and/or civil penalties.

c. The process must be described in access agreements.

d. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions.

Note: The process can be included as part of the general personnel policies and procedures for the organization.

7. RELATED DOCUMENTS

- NIST SP 800-35, *Guide to Information Technology Security Services*, October 2003
- NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009
- 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
- Intelligence Community Directive 704, *Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information,* October 2008

8. ROLES AND RESPONSIBILITIES

Office of Administration and Resources Management (OARM)

a. OARM has the following responsibilities with respect to personnel security:

i. Coordinate with IT management and staff in arriving at the appropriate risk and sensitivity designation for positions and functions.

ii. Designate a final risk/sensitivity level based on the Program or Regional Office designation, position risk points, and adjustments.

iii. Notify the requesting Program or Regional Office of background investigation status and results.

iv. Coordinate with and provide advice and assistance to IT management and staff in establishing appropriate sanctions.

v. Ensure employee separation and transfer forms and checklists account for required information systems access changes.

Office of General Counsel (OGC)

a. OGC has the following responsibilities with respect to personnel security:
    i. Provide advice and assistance to OARM and Program and Regional Office management and staff on appropriate sanctions and potential legal penalties.

Contracts Officer, Project Officer, and Contracting Officer Technical Representative (COTR)

a. The Contracts Officer, Project Officer, and COTR have the following responsibilities with respect to personnel security:
    i. Ensure that contractors and other third-party service providers are subject to the same personnel screening requirements as EPA personnel.
    ii. Ensure required agreements and sanctions are developed and appropriate language and forms are in the contract or grant documents.
    iii. Ensure there is a procedure to handle contract or grantee terminations and other changes such as transfers to address required information system access changes.

Program and Regional Offices

a. The Program and Regional Offices have the following responsibilities with respect to personnel security:
    i. Initiate the risk designation process as required.
    ii. Provide funding for background screening and clearances.

Senior Information Official (SIO)

a. The SIO has the following responsibilities with respect to personnel security:
    i. Ensure sufficient funding for background screening and clearances as required.
    ii. Certify that personnel security is in compliance with termination procedures; the certifying statements must be kept on file.
    iii. Certify that personnel security is in compliance with transfer procedures.

System Owner (SO)

a. The SO has the following responsibilities with respect to personnel security:
    i. Provides procurement, development, integration, modification, operation, maintenance, and disposal of an information system.Provides operational interests of the user community (i.e., users who require access to the

information system to satisfy mission, business, or operational requirements)Provides the development and maintenance of the security plan and ensures that the system is deployed and operated in accordance with the agreed-upon security controls.Responsible for deciding who has access to the system (and with what types of privileges or access rights) and ensures that system users and support personnel receive the requisite security training (e.g., instruction in rules of behavior)

ii. Reviews security assessment results from the Security Control Assessor

Personnel Specialists

a. Personnel specialists have the following responsibilities with respect to personnel security:

i. Ensure information related to risk and sensitivity of positions is complete on all personnel actions and in accordance with the “Position Risk Designation and Background Investigation” procedure, June 2010.

ii. Notify appropriate IT and information management and staff on personnel actions that impact security of and access to information systems (e.g., terminations, transfers).

Information Security Officer (ISO)

a. The ISO have the following responsibilities with respect to personnel security:

i. Identify positions and functions requiring background screening and clearances for their information systems.

ii. Develop personnel security requirements for staff and contracts.

iii. Implement personnel security requirements for their information systems.

iv. Define and document operational procedures to verify that any information system user with a temporary or interim account successfully completes the screening process before the account is changed to a standard/non-temporary account.

Information System Security Officer (ISSO)

a. The ISSO has the following responsibilities with respect to personnel security:

i. Assist the SO and ISO in their responsibilities.

ii. Review agreements and contracts for personnel security requirements.

9. DEFINITIONS

- Involuntary Termination - the employee's departure at the decision of the employer. There are two basic types of involuntary termination, often referred to as being "fired" and "laid off." To be fired, as opposed to being laid off, is generally thought to be the employee's fault, and is, therefore, typically considered to be dishonorable and a sign of failure. Being laid off is a result of an organization’s strategic, operational, or financial decision; and such a decision usually affects multiple employees through no fault of their own.

- 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.
- Voluntary Termination - a decision made by the employee to leave the job. Such a decision is commonly known as "resignation,” "quitting,” "leaving,“ or "giving notice.”
- 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 POLICIES, STANDARDS AND GUIDANCE

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, Section 10.1

13. ADDITIONAL INFORMATION

NA

EPA Classification No.:	CIO-2150.3-P-13.1	CIO Approval Date:	08/06/2012
CIO Transmittal No.:	12-003	Review Date:	08/06/2015

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

APPENDIX A: ACRONYMS

CIO	Chief Information Officer
COTR	Contracting Officer Technical Representative
EPA	Environmental Protection Agency
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GSS	General Support Schedule
ISO	Information Security Officer
ISSO	Information System Security Officer
IT	Information Technology
LBI	Limited Background Investigation
MA	Major Application
NIST	National Institute of Standards and Technology
OARM	Office of Administration and Resources Management
OEI	Office of Environmental Information
OIG	Office of Inspector General
OGC	Office of General Counsel
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PIV	Personal Identity Verification
RCRA	Resource Conservation and Recovery Act
SAISO	Senior Agency Information Security Officer
SCI	Special Compartment Information
SIO	Senior Information Official
SO	System Owner
SP	Special Publication
USC	United States Code

DOCUMENT CHANGE HISTORY

Version	Release Date	Summary of Changes	Author of Changes	DCN
0.5	2/16/2009	Initial draft	Heather Flager	Procedures-PS-Draft_TO62_020_1
1.0	6/26/2009	Incorporated EPA comments Final	Heather Flager	Procedures-PS-Final_TO62_020_2
1.7	8/9/2010	Updated per NIST SP 800-53 Rev 3	Heather Flager	Procedures_PS_Draft.TO-062_050_1.0
1.7	8/19/2010	TISS Initial comments and reviews	Charleen Johnson	Procedures_PS_Draft.TO-062_050_1.0
1.8	1/12/2010	TISS Final Draft Review	Charleen Johnson	Procedures_PS_Draft.TO-062_050_1.0
1.9	4/20/2012	SAISO Final Review	Abe Getchell & Jabran	Procedures_PS_Draft.TO-062_050_1.0
2.0	7/18/2012	Document Review	LaToya Gordon	Procedures_PS_Draft.TO-062_050_1.0