EPA Classification No.:	CIO-2150.3-P-11.1	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 PHYSICAL AND ENVIRONMENTAL PROTECTION PROCEDURES
V1.9
MAY 4, 2012

1. PURPOSE

The purpose of this procedure is to facilitate the implementation of Environmental Protection Agency (EPA) security control requirements for the Physical and Environmental Protection 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 physical and environmental protection 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)
- Office of Management and Budget (OMB) Memorandum M-05-24, "*Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*", August 2005
- OMB Memorandum M-06-06, "*Sample Privacy Documents for Agency Implementation of Homeland Security Presidential Directive (HSPD) 12"*, February 2006
- OMB Memorandum M-06-18, "*Acquisition of Products and Services for Implementation of HSPD-12*", June 2006
- OMB Memorandum M-07-06, "*Validating and Monitoring Agency Issuance of Personal Identity Verification Credentials*", January 2007
- OMB Memorandum M-08-01, "*HSPD-12 Implementation Status*", October 2007
- OMB Circular A-130, "*Management of Federal Information Resources*", Appendix III, "*Security of Federal Automated Information Resources*", November 2000
- 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, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, March 2006
- EPA Information Security Program Plan
- EPA Information Security Policy
- EPA Delegations 1-4-B. Real Property and Space
- EPA Delegations 1-84. Information Resources Management

6. PROCEDURES

PE- 2 – Physical Access Authorizations

a. Access to EPA buildings, rooms, work areas, spaces, and structures housing information systems, equipment, and data shall be limited to authorized personnel.

b. Reviews and approves the access list and authorization credentials quarterly.

c. A current list of personnel with authorized access to the facility or designated area within a facility where the information system resides must be kept.

   i. Those areas within the facility officially designated as publicly accessible are exempt from this requirement.

d. Authorization credentials (e.g., badges, identification cards, and smart cards) must be issued.

   i. The level of access provided to each individual must not exceed the level of access required to complete the individual’s job responsibilities.

      ▪ The level of access must be reviewed and approved.

   ii. Keys, badges, access cards, and combinations must be issued to only those personnel who require access.

   iii. Authorizations and requirements for access must be coordinated with facility and personnel security managers, as required or needed.

e. Access lists and authorization credentials must be reviewed and approved weekly to ensure the following:

   i. Access must be limited to only authorized personnel.

   ii. The level of access provided to each individual must be consistent with the individual’s job responsibilities.

   iii. Access rights must be promptly removed for terminated and transferred personnel or for personnel no longer requiring access to the facility where the information system resides.

      - Coordination must occur with human resources for EPA employees.
      - Coordination must occur with contract and grant management personnel for contractors and grantees.

PE-3 – Physical Access Control

a. Physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides must be enforced.

   i. Those areas within the facilities officially designated as publicly accessible may be excluded from this requirement, in accordance with established physical security requirements.

   ii. Access to areas officially designated as publicly accessible must be controlled in accordance with the assessment of risk.

b. Individual access authorizations must be verified before access to the facility is granted.

c. Inventories physical devices quarterly.

d. Physical access devices (e.g., keys, locks, combinations, card readers) and/or guards must be used to control entry to facilities containing information systems.

i. Stringent key and combination controls must be implemented at the facilities or designated areas within facilities, as applicable to ensure physical access protections.

ii. Physical access devices (e.g., keys, locks, combinations, card readers used at the Agency) must be functioning properly.

- Maintenance on these devices must occur on a regular and scheduled basis.

Note: The organization determines the types of guards needed (e.g., professional physical security staff or other personnel, such as administrative staff or information system users as deemed appropriate).

e. Keys, combinations, and other physical access devices must be secured and inventoried annually.

i. Coordination with facility management personnel must occur, where applicable.

f. Combinations and keys must be changed on a routine basis.

i. In addition, combinations and keys must be changed immediately for reasons such as:

- Keys are lost.
- Combinations are compromised.
- Individuals are transferred, terminated, or no longer need access.
- There is a theft or security violation in the area being protected.

ii. Coordination must occur with facility management personnel, as required.

g. All individuals accessing EPA facilities must have an authorized EPA identification badge or visitor's badge.

i. All EPA personnel and visitors are required to display their badges.

h. After an emergency-related event, reentry to facilities must be restricted to authorized individuals only.

i. All equipment that stores, processes, or transmits EPA information must be located in an appropriate locked rack, room, or enclosure.

i. Workstations and associated peripherals connected to (and part of) an information system may be located in areas designated as publicly accessible, with access to such devices being safeguarded in accordance with EPA's assessment of risk.

j. Protocol analyzers and other devices capable of reading and decoding data transmitted on the network must be kept in a locked, limited-access compartment or room.

i. Only authorized personnel shall have access to these devices.

ii. These devices must remain locked up except when in use.

k. All physical access control deficiencies must be entered into the Plan of Action and Milestones (POA&M) of the Agency's FISMA reporting and tracking system if the deficiencies are not corrected within 30 days for high-level risks or 60 days for moderate-level risks.

    i. Refer to *Information Security – Interim Security Assessment and Authorization Procedures* for requirements on POA&Ms.

l. NIST SP 800-73-3 must be used for requirements for Personal Identity Verification (PIV) interfaces.

m. NIST SP 800-76-1 must be used for requirements on PIV biometric data specifications.

n. NIST SP 800-78-2 must be used for requirements on PIV cryptographic algorithms and key sizes.

For high information systems

o. Physical access authorizations to the information system must be enforced independent of the physical access controls for the facility.

    i. This requirement applies to server rooms, media storage areas, communications centers, or any other areas within an organizational facility containing large concentrations of information system components.

Note: The intent is to provide additional physical security for those areas where the organization may be more vulnerable due to the concentration of information system components.

    ii. This requirement applies to the information system and security control consoles.

p. Security requirements for facilities containing organizational information systems that process, store, or transmit Sensitive Compartmented Information (SCI) must be consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

<u>PE-4 – Access Control for Transmission Medium</u>

For moderate and high information systems

a. Physical access to information system distribution and transmission lines within organizational facilities must be controlled.

Note: Physical protections applied to information system distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Additionally, physical protections are necessary to help prevent eavesdropping or modification of unencrypted transmissions while in transit.

b. Protective measures to control physical access to information system distribution and transmission lines must include the following:

i. Locked wiring closets.

ii. Disconnected or locked spare jacks.

iii. Protection of cabling by conduit or cable trays.

PE-5 – Access Control for Output Devices

For moderate and high information systems

a. Physical access to information system output devices (e.g., monitors, printers, audio devices) must be controlled to prevent unauthorized individuals from obtaining the output.

i. Methods to protect display devices include repositioning the monitor, and/or using a monitor filter.

PE-6 – Monitoring Physical Access

a. Physical access to the information system must be monitored to detect and respond to physical security incidents.

i. Coordination with facility management and personnel security management personnel must occur when responsibilities are in different organizations.

b. Physical access logs must be reviewed monthly.

c. Investigations of apparent security violations or suspicious physical access activities must be conducted. Investigations and results of reviews must be coordinated with the organization’s incident response capability.

i. Remedial actions identified as a result of investigations must be developed and implemented.

ii. Refer to *Information Security – Interim Incident Response Procedures* for requirements on incident response.

d. Investigation of and response to detected physical security incidents, including apparent security violations or suspicious physical access activities must be part of the organization’s incident response capability.

i. Individuals who have physical protection response responsibilities must be identified in writing.

ii. Operational procedures must be developed to document how these individuals shall respond to physical access incidents.

For moderate and high information systems

e. Real-time physical intrusion alarms and surveillance equipment must be installed and monitored.

For high information systems

f. Automated mechanisms to recognize potential intrusions and initiate designated response actions must be employed.

g. Reviews physical access logs weekly.

PE-7 – Visitor Control

a. Physical access to the information system must be controlled by authenticating visitors before authorizing access to the facility where the information system resides.

   i. Requirements must be coordinated with facility management personnel.

   ii. Authentication and authorization to access areas other than those designated as publicly accessible must be in accordance with facility management requirements and facility risk assessments.

Note: Individuals (to include organizational employees, contract personnel, and others) with permanent authorization credentials for the facility are not considered visitors; however, persons are considered visitors when their clearance status is unknown.

b. Police, fire, or Emergency Medical Services (EMS) personnel responding to an emergency call from EPA or building management may deviate from any part of the requirements in this procedure that inhibits their emergency response efforts.

   i. Police, fire, or EMS personnel must be in uniform or show an identification badge before entering facilities where EPA information systems are located.

   ii. EPA or building security guards must accompany all police, fire, or EMS to all incidents to assist the emergency personnel with locating the source of the call and to verify that it is a legitimate incident and not a diversion.

For moderate and high information systems

c. Visitors must be escorted and visitor activity must be monitored.

d. Visitors must provide two forms of identification to gain access to the facility

e. Visitors requiring access to controlled information system processing areas must be escorted.

   i. All visitors shall sign a visitor log.

   ii. Information system maintenance and repair personnel must be categorized as visitors unless they are classified as EPA contractors and have EPA identification badges.

<u>PE-8 – Access Records</u>

a. Visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) must be maintained.

b. The visitor access record must address the following components:

   i. Name and organization of the person visiting.

   ii. Signature of the visitor.

   iii. Form(s) of identification.

   iv. Date of access.

   v. Time of entry and departure.

vi. Purpose of visit.

vii. Name and organization of person visited.

c. The visitor access records must be reviewed twice a year.

For high information systems

d. Automated mechanisms must be employed to facilitate the maintenance and review of access records.

e. A record of all physical access, both visitor and authorized individuals, must be maintained.

f. Reviews visitor access logs weekly.

PE-9 – Power Equipment and Power Cabling

Note: This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

For moderate and high information systems

a. Power equipment and power cabling for the information system must be protected from damage and destruction.

b. Power cabling must be inspected annually for the following:

   i. Power cables under raised floors and in drop ceilings must be inspected for fraying or other wear, such as damage from water or pest infestation.

   ii. Facilities with hangers and trays that support power cables must be inspected for stability.

c. The results of the inspection must be documented to include the following:

   i. Date(s) of inspection.

   ii. Person(s) conducting inspection(s).

   iii. Location(s) inspected.

   iv. Component(s) inspected.

   v. Inspection results.

d. All deficiencies must be entered into the Agency's FISMA reporting and tracking system as POA&Ms if the deficiencies are not corrected within 30 days for high-level risks or 60 days for moderate-level risks.

   i. Refer to *Information Security – Interim Security Assessment and Authorization Procedures* for requirements on POA&Ms.

e. Automatic voltage controls must be in place for all critical information system.

   i. At a minimum, all server equipment.

PE-10 – Emergency Shutoff

Note: This control applies to facilities containing concentrations of information system *resources, for example, data centers, server rooms, and mainframe computer rooms.*

For moderate and high information systems

- The capability must be provided to shut off power to the information system or individual system components in emergency situations.
  - i. Coordination must occur with facilities management personnel, as needed or required.
- Emergency shutoff switches or devices must be placed in locations as defined by applicable standards to facilitate safe and easy access for personnel. Refer to NFPA 70.
- An emergency shutoff or shutdown operational procedure must be documented. The procedure, at a minimum, must include the following:
  - i. Whether the information system component is capable of an emergency shutoff.
  - ii. Notification of personnel when an emergency shutoff is recommended or executed.
  - iii. Detailed steps for an emergency shutoff.
  - iv. Maximum time allotted for the emergency shutoff.
- The locations for emergency power shutoffs must be documented.
- All necessary personnel must be informed of the emergency power shutoff locations and they must be trained to operate them safely.
- Emergency procedures must be readily available to relevant personnel.
- The emergency power-off capability must be protected from accidental or unauthorized activation.
- Emergency shutoff switches are located in a visible location and clearly labeled.

<u>PE-11 – Emergency Power</u>

Note: This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

For moderate and high information systems

a. A short-term Uninterruptible Power Supply (UPS) must be provided to facilitate an orderly shutdown of the information system in the event of a primary power source loss.
   - i. The UPS must be tested monthly.

b. Each office shall provide for uninterrupted and functioning ties that include, but are not limited to, the following:
   - i. There must be some form of uninterruptible power source to provide electricity for emergency system shutdowns, and surge protectors to secure

against power fluctuations.

ii. Servers and critical hardware devices must be protected by a UPS, installed either centrally or locally.

iii. Workstations must be protected from power surges through the installed electrical wiring of the building or through external surge protectors.

For high information systems

c. A long-term alternate power supply that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source must be provided for the information system.

i. Acceptable long-term alternate power supplies include a battery system with rectifiers, generators, etc.

ii. The long-term alternate power supply selected must be able to support the documented availability requirements for the information system.

iii. The long-term alternate power supply must be documented in the Contingency Plan for the information system.

- Refer to *Information Security – Interim Contingency Planning Procedures* for requirements on Contingency Plans.

d. A major application that is categorized as high must ensure that systems providing processing support (e.g., general support systems) have sufficient alternative power supply capabilities for their requirements.

i. The Contingency Plans for both the major application and the general support systems must reflect these requirements.

e. Emergency power capabilities must be tested periodically but at least annually.

i. Tests must be conducted prior to seasons of expected events (e.g., prior to hurricane season) to ensure effective operation, if needed.

PE-12 – Emergency Lighting

Note: This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

a. Automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility must be employed and maintained.

b. The automatic emergency lighting systems must be tested annually to ensure they are fully operational.

i. The results of the test must be documented.

PE-13 – Fire Protection

Note: This control, to include any enhancements specified, may be satisfied by similar *requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.*

a. Fire suppression and detection devices/systems for the information system that are supported by an independent energy source must be employed and maintained.

Note: Fire suppression and detection devices/systems include, for example, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors.

b. Fire extinguishers must be checked annually and the inspection date must be documented on the extinguisher.
c. All server/computer rooms or data centers must have at least one hand-held fire extinguisher that it easily accessible.
d. Personnel must be trained on how to use a fire extinguisher and must receive annual refresher training.
e. All fire protection resources must be tested annually in accordance with local or state fire regulations to ensure they can be successfully activated in the event of a fire.

For moderate and high information systems

f. Fire detection devices/systems for the information system that activate automatically in the event of a fire must be employed.
g. Fire detection devices/systems for the information system must notify the organization and emergency responders in the event of a fire.
h. Fire suppression devices/systems for the information system that provide automatic notification of any activation to the organization and emergency responders must be employed.
i. An automatic fire suppression capability for the information system must be employed when the facility is not staffed on a continuous basis.
j. Contingency Plans must account for suppression system impacts on the system components and plan accordingly.
    i. Refer to *Information Security – Interim Contingency Planning Procedures* for requirements on Contingency Plans.

PE-14 –Temperature and Humidity Controls

Note: This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

a. The temperature and humidity levels within the facility where the information system resides must be maintained within limits as required by the equipment being protected.

b. The temperature and humidity levels within the facility where the information system resides must be monitored real time; continuously.

PE-15 – Water Damage Protection

Note: This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

a. The facility must have master shutoff valves that are accessible, working properly, and known to key personnel, in order to protect the information system from damage resulting from water leakage.

For high information systems

b. Mechanisms must be employed that, without the need for manual intervention, protect the information system from water damage in the event of a water leak.

PE-16 – Delivery and Removal

a. Any and all types of information system components and packages that are delivered to or removed from the facility must be authorized, monitored, and controlled.
b. Records of those items entering and exiting the facility must be maintained.
c. Delivery areas must be restricted access areas and possibly isolated from the information system and media libraries in order to effectively enforce authorizations for entry and exit of information system components.
    i. Refer to *Information Security – Interim Media Protection Procedures* for further information on media protection.

PE-17 – Alternate Work Site

For moderate and high information systems

a. Management, operational, and technical information system security controls must be employed at alternate work sites.
    i. The alternate work site must have protection equivalent to the primary work environment.

Note: Alternate work sites may include, for example, government facilities or private residences of employees. The organization may define different sets of security controls for specific alternate work sites or types of sites.

b. The effectiveness of security controls at alternate work sites must be assessed, as feasible.
c. A means (e.g., phone numbers) for employees to communicate with information

security personnel in case of security incidents or problems must be provided.

d. An alternate work site must be available for business resumption activities in case of a disaster.

e. Equipment being used or stored at an individual alternate work site, such as hotel, home, or other alternate site, must be secured when not in use.

   i. Equipment stored in vehicles must be hidden from casual view.

   ii. Equipment must not be stored in vehicles overnight.

f. Users shall adhere to the following in regards to working in a flexiplace environment:

   i. Comply with all requirements of the information system and those in the Rules of Behavior.

   ii. Ensure access to applicable contact information for reporting suspicious activity.

   iii. Comply with the applicable personnel, software, copyright, and licensing agreements related to the flexiplace environment, including the use of confidentially sensitive data.

   iv. Ensure that the computer and remote access capabilities provided by EPA are used for authorized activities only.

   v. Protect equipment and media (i.e., digital, non-digital) from damage and unauthorized access.

      - Refer to *Information Security – Interim Media Protection Procedures* for further information on media protection.

   vi. Ensure that the remote office area is not subject to excess moisture (e.g., damp basement) or flooding.

   vii. Use a surge protector.

   viii. Use Agency-approved flaw remediation software to scan all electronic data storage and remote files for viruses before accessing them.

      - Refer to *Information Security – Interim System and Information Integrity Procedures* for further information on flaw remediation.

   ix. Virus protection software must be installed and operational at all times.

   x. Store files to the EPA home server when possible or back up data on a weekly basis in an approved manner.

g. NIST SP 800-46, Revision 1 must be used as guidance for security in telework and remote access.

PE-18 – Location of Information System Components

Note: This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

For moderate and high information systems

a. Information system components must be positioned within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.

   i. Examples of minimizing potential damage by careful positioning include these:

      - In an earthquake zone, an unanchored/untethered storage cabinet should not be placed next to critical equipment, lest it fall over and damage the equipment.
      - If water pipes are running overhead, then cabling or equipment should not be placed underneath the pipes.

Note: Physical and environmental hazards include, for example, flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electromagnetic pulse, electrical interference, and electromagnetic radiation.

b. The location or site of the facility must be considered with regard to physical and environmental hazards.

c. The location of physical entry points where unauthorized individuals, while not being granted access, might nonetheless be in close proximity to the information system and therefore, increase the potential for unauthorized access to organizational communications (e.g., through the use of wireless sniffers or microphones) must be considered.

For high information systems

d. The location or site of the facility where the information system resides must be planned with regard to physical and environmental hazards.

e. For existing facilities, the physical and environmental hazards must be considered in the risk mitigation strategy for the information system.

7. RELATED DOCUMENTS

- 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 800-73-3, *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

8. ROLES AND RESPONSIBILITIES

Office of Administration and Resource Management (OARM) and Local Facility and Health and Safety Management Officials

a. The responsible OARM and related local facility and health and safety managers have the following responsibilities with respect to physical and environmental protection for information system and related facility requirements:

i. Coordinate with System Owners (SOs) on planning, implementation and needed improvements to physical and environmental controls at facilities.

ii. Ensure that physical and environmental controls systems and installations meet applicable federal and local operational and safety standards as applicable.

iii. Coordinate with SOs and Senor Information Management Officials (IMOs) on an ongoing basis.

iv. Ensure appropriate, responsible personnel are assigned to conduct reviews for relevant PE controls for the annual FISMA review and certification requirements, as required.

Senior Information Official (SIO)

b. The SIO has the following responsibilities with respect to physical and environmental protection:

i. Facilitate coordination and implementation of required controls with OARM and local senior management, as needed.

ii. Ensure adequate funding is planned and provided to meet requirements.

Information Management Officer (IMO)

c. The IMO has the following responsibilities with respect to physical and environmental protection:

i. Ensure that programmatic or Regional requirements, as appropriate, are consolidated and coordinated, as needed.

ii. Raise unresolved issues and funding needs to senior management.

iii. Consolidate plans and budgetary requirements to ensure cost-effective, timely, and efficient implementation off requirements.

System Owner (SO)

d. The SO has the following responsibilities with respect to physical and environmental protection:

i. Comply with Agency policies and procedures for physical and environmental controls pertaining to facilities where information systems and components reside and designated areas.

ii. Determine specific physical and environmental control requirements for their information systems facilities and designated areas.

iii. Coordinate with local facilities and health and safety managers regarding planning, implementation, and improvement of the control requirements, needs for existing facilities, and moves to new or different facilities.

iv. Ensure POA&Ms are planned, entered into the Agency's FISMA reporting and tracking system, completed, and implemented as required by deficiency findings and reviews.

v. Ensure appropriate responsible personnel are assigned to conduct reviews for relevant PE controls for the annual FISMA review and certification requirements.

Information System Security Officer (ISSO)

e. The ISSO has the following responsibilities with respect to physical and environmental protection:

i. Implement the operational aspects of the SO's responsibilities.

ii. Assist SOs and managers in responsibilities for planning, reviewing and implementing required controls.

Users / Individuals

f. Users/individuals have the following responsibilities with respect to physical and environmental protection:

i. Adhere to the Agency and information system policy, procedures, and rules of behavior in regards to physical and environmental protection and controls for working in a flexiplace environment.

9. DEFINITIONS

- Alternate Work Site – a location other than the official duty station that has been approved by the personnel's supervisor (e.g., residence, satellite office, flexiplace) in order to perform job duties.
- Electronic Data Storage – storage which requires electrical power to store and retrieve that data.
- Fire Detection Systems – systems that are used to protect and evacuate people in emergencies. Examples include fire alarms, smoke, heat, and carbon monoxide detectors, voice evacuation and mass notification systems, and emergency lighting systems.
- Fire Suppression Systems – systems that are used in conjunction with smoke detectors and fire alarms to suppress a fire. Examples include wet and dry sprinkler systems, fire extinguishers, and dry chemical, foam, and gaseous extinguishing agents.
- Flexiplace (Flexible Workplace) – employment at a location such as a satellite location or employee residence during an agreed-upon portion of an individual's workweek.
- 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, Section 11.2.4

13. ADDITIONAL INFORMATION

NA

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

APPENDIX A: ACRONYMS

CIO	Chief Information Officer
EPA	Environmental Protection Agency
EMS	Emergency Medical Services
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
HSPD	Homeland Security Presidential Directive
IMO	Information Management Officer
ISSO	Information System Security Officer
IT	Information Technology
NIST	National Institute of Standards and Technology
OARM	Office of Administration and Resources Management
OMB	Office of Management and Budget
PIV	Personal Identity Verification
POA&M	Plan of Action and Milestones
SAISO	Senior Agency Information Security Officer
SCI	Sensitive Compartmented Information
SIO	Senior Information Official
SO	System Owner
SP	Special Publication
UPS	Uninterruptible Power Supply
USC	United States Code

DOCUMENT CHANGE HISTORY

Version	Release Date	Summary of Changes	Author of Changes	DCN
0.5	1/29/2008	Initial draft	Heather Flager	Procedures-PE-Draft_TO62_020_1
1.0	6/17/2009	Incorporated EPA comments Final	Heather Flager	Procedures-PE-Final_TO62_020_2
1.7	8/11/2010	Updated per NIST SP 800-53 Rev 3	Heather Flager	Procedures_PE_Draft.TO-062_050_1.0
1.8	12/27/2010	TISS Final Draft Review	Charleen Johnson	Procedures_PE_Draft.TO-062_050_1.0
1.9	5/4/2012	SAISO Final Review	Abe Getchell & Jabran	Procedures_PE_Draft.TO-062_050_1.0
1.8	7/18/2012	Document Review	LaToya Gordon	Procedures_PE_Draft.TO-062_050_1.0