INFORMATION DIRECTIVE
INTERIM PROCEDURE

Information Security – Interim Physical and Environmental Protection Procedures		
Directive No.: 2150-P-11.2	CIO Approval: 12/30/2016	Transmittal No.: 17-004d

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

Information Security – Interim Physical and Environmental Protection Procedures

1. PURPOSE

To extend and provide specificity to the Environmental Protection Agency (EPA) Information Security Policy. This document shall be used to develop procedures, standards and guidance that facilitate the implementation of security control requirements for the Physical and Environmental Protection (PE) control family, as identified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

2. SCOPE

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

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 the EPA.

3. AUDIENCE

The audience is all EPA employees, contractors and all other users of EPA information and information systems that support the operations and assets of the EPA.

4. BACKGROUND

Based on federal requirements and mandates, the EPA is responsible for ensuring 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 shall meet the security requirements through the use of the security controls defined in the NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. This document addresses the procedures and standards set forth by the EPA and complies with the Physical and Environmental Protection family of controls.

5. AUTHORITY

The information directive is issued by the EPA Chief Information Officer (CIO), Pursuant to Delegation 1-19, dated 07/07/2005.

Additional legal foundations for the procedure include:

- Federal Information Security Modernization Act (FISMA) of 2014, Public Law 113-283, chapter 35 of title 44, United States Code (U.S.C.)
- E-Government Act of 2002, Public Law 107-347, Title III, Federal Information Security Management Act, 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 U.S.C. 3501-3519)
- Privacy Act of 1974 (5 U.S.C. § 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
- 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
- NIST SP 800-12, An Introduction to Computer Security – The NIST Handbook, October 1995
- NIST SP 800-30, Revision 1, Guide for Conducting Risk Assessments.

- NIST SP 800-46, Revision 1, Guide to Enterprise Telework and Remote Access Security
- NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-73-3 PIV Interfaces
- NIST SP 800-76-1 PIV Biometric Data Specifications.
- NIST SP 800-78-2 PIV Cryptographic Algorithms and Key Sizes
- NIST SP 800-114, User's Guide to Securing External Devices for Telework and Remote Access
- NIST SP 800-121, Guide to Bluetooth Security
- 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
- EPA Information Security Roles and Responsibilities Procedures
- EPA Flexiplace Policy 3180
- EPA Information Security Continuous Monitoring Strategic Plan
- CIO Policy Framework and Numbering System

6. PROCEDURE

The "PE" designator identified in each procedure represents the NIST-specified identifier for the Physical and Environmental Protection control family, as identified in NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

PE-1 – Physical and Environmental Protection Policy and Procedures

1) System Owners (SO), in coordination with the Office of Administration and Resources Management (OARM), local building management (e.g., Facility, Health and Safety Management Officials), and Senior Information Officials (SIO), for EPA-operated systems, shall; and Service Managers (SM), in coordination with Information Management Officers (IMO), for systems operated on behalf of the EPA, shall ensure service providers:

a) Develop a physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment and coordination among organizational entities and compliance.

b) Develop procedures to facilitate the implementation of the physical and environmental protection policy, associated physical and environmental protection policy and associated physical and environmental protection controls.

PE-2 – Physical Access Authorizations

Note: This control addresses individuals'[1] access to buildings, rooms, work areas, spaces and structures housing EPA information and information systems. This control only applies to facilities and areas within facilities that have not been designated as publicly accessible. This control applies to organizational employees and visitors.

1) SOs, in coordination with OARM, local building management (e.g., Facility, Health and Safety Management Officials), and SIOs, for EPA-operated systems, shall; and SMs, in coordination with IMOs, for systems operated on behalf of the EPA, shall ensure service providers:[2]
   a) Develop, approve and maintain a current list of personnel with authorized access to the facility or designated areas within a facility where EPA information is processed or stored.
      i) The level of access provided to each individual shall not exceed the level of access required to complete the individual's job responsibilities.
      ii) The level of access shall be reviewed and approved by the SO or Information Owner (IO) as appropriate.
   b) Issue authorization credentials (e.g., keys, badges, identification cards, access cards and smart cards) for access.
      i) Authorizations and requirements for access shall be coordinated with facility and personnel security managers, as required.
      ii) Keys, badges, access cards and combinations shall be issued to only those personnel who require access.
   c) Review and approve the access list detailing authorized facility access by individuals at least quarterly to ensure:
      i) Individuals to whom the authorization credentials were issued still require them.
      ii) Issued authorization credentials do not exceed the level of access required by the assigned individual's current job responsibilities.
   d) Remove individuals from access lists when access is no longer required.

PE-2(1) – Physical Access Authorizations | Access by Position / Role

Not selected as part of the control baseline.

PE-2(2) – Physical Access Authorizations | Two Forms of Identification

Not selected as part of the control baseline.

[1] *Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors.*

[2] *Service Providers' controls are validated through independent assessments in accordance with Federal Risk and Authorization Management Program (FedRAMP). Information Owners and Service Managers ensure controls are in place and operating as intended by reviewing documentation provided by Service Providers and FedRAMP. Authorizing Officials may accept provisional authorizations to operate issued by FedRAMP as a result of review by the combined Department of Defense (DoD), General Services Administration (GSA), & Department of Homeland Security (DHS) process without reviewing supporting documentation. Supporting documentation for all other provisional authorizations to operate shall be reviewed before acceptance.*

PE-2(3) – Physical Access Authorizations | Restrict Unescorted Access

Not selected as part of the control baseline.

PE-3 – Physical Access Control

For All Information Systems:

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.

1) SOs, in coordination with OARM, local building management (e.g., Facility, Health and Safety Management Officials), and SIOs, for EPA-operated systems, shall; and SMs, in coordination with IMOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Enforce physical access authorizations for all physical access points to non-public facilities and areas where EPA information is stored or processed by:
      i) Verifying individual access authorizations before granting access.
      ii) Controlling ingress/egress using physical access controls such as guards, and keyed, combination or electronic locks.
         (1) All authorized personnel and visitors are required to display their badges while inside the facility.
         (2) All visitors shall sign a visitor log and be escorted by an employee while in non-public areas.
      iii) Ensuring that all equipment that stores, processes or transmits EPA information is located in an appropriate, access controlled space.
         (1) Components of an information system may be placed and operated in areas designated as publicly accessible when they are adequately protected in accordance with a risk assessment.[3]
   b) Maintain physical access audit logs for designated entry/exit points to non-public spaces where EPA information is processed or stored.
      i) Audit logs can be manual or automated.
   c) Ensure keys, combinations and other physical access devices are secured.
      i) Change locks when they no longer adequately deter unauthorized access and change combinations and keys when keys are lost or otherwise unaccounted for and when combinations are compromised or individuals are transferred or terminated.
   d) Inventory keys annually, as well as when:
      i) Keys are lost;
      ii) Individuals are transferred or terminated;
      iii) Replacement keys are issued;
      iv) There is a theft or security violation in the protected area.
   e) Develop a Plan of Action and Milestones (POA&M) for all physical access security control deficiencies and enter it into the Agency's Information Security Repository in accordance with POA&M reporting procedures.[4]

[3] *The Risk Management Framework is described in draft NIST SP 800-39, Managing Risk from Information Systems: An Organizational Perspective.*

[4] *Document the results of security control test(s), [Deficiencies/Weaknesses] in the Agency Information Security Repository, the Agency's tool for managing POA&Ms, and create a POA&M finding.*

i) Refer to Information Security – Security Assessment and Authorization Procedures for POA&M requirements identified in Appendix B, POA&M Monitoring and Validation Process Diagram and Outline and Table 1, Process Outline.

PE-3(1) – Physical Access Control | Information System Access

For High Information Systems:

Note: This control enhancement provides additional physical security for those areas within facilities where there is a concentration of information system components (e.g., server rooms, media storage areas, data and communications centers).

1) SOs, in coordination with OARM, local building management (e.g., Facility, Health and Safety Management Officials), and SIOs, for EPA-operated systems, shall; and SMs, in coordination with IMOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Enforce physical access authorizations to the information and information system and physical access controls for the facility at physical spaces containing one or more components of the information system (e.g., network/communication closets and rooms).
      i) This requirement applies to the information system and security control consoles.

PE-3(2) – Physical Access Control | Facility / Information System Boundaries

Not selected as part of the control baseline.

PE-3(3) – Physical Access Control | Facility / Continuous Guards / Alarms / Monitoring

Not selected as part of the control baseline.

PE-3(4) – Physical Access Control | Facility / Lockable Casings

Not selected as part of the control baseline.

PE-3(5) – Physical Access Control | Facility / Tamper Protection

Not selected as part of the control baseline.

PE-3(6) – Physical Access Control | Facility / Facility Penetration Testing

Not selected as part of the control baseline.

PE-4 – Access Control for Transmission Medium

For Moderate and High Information Systems:

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.

1) SOs, in coordination with OARM, local building management (e.g., Facility, Health and Safety Management Officials), and SIOs, for EPA-operated systems, shall; and SMs,

in coordination with IMOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Control physical access to information system distribution and transmission lines using security safeguards, such as, locked wiring closets and cable trays or conduit.

PE-5 – Access Control for Output Devices

For Moderate and High Information Systems:

Note: Methods to control and protect physical access to output devices include placing output devices in locked rooms or other secured areas and allowing access to authorized individuals only, placing output devices in locations that can be monitored by organizational personnel or repositioning the output device and/or using a privacy screen for the output device.

1) SOs, in coordination with OARM, local building management (e.g., Facility, Health and Safety Management Officials), and SIOs, for EPA-operated systems, shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Control physical access to information system output devices (e.g., monitors, printers, copiers, scanners, facsimile machines and audio devices) to prevent unauthorized individuals from obtaining the output.

PE-5(1) – Access Control for Output Devices | Access to Output by Authorized Individuals

Not selected as part of the control baseline.

PE-5(2) – Access Control for Output Devices | Access to Output by Individual Identity

Not selected as part of the control baseline.

PE-5(3) – Access Control for Output Devices | Marking Output Devices

Not selected as part of the control baseline.

PE-6 – Monitoring Physical Access

For All Information Systems:

1) SOs, in coordination with OARM, local building management (e.g., Facility, Health and Safety Management Officials), and SIOs, for EPA-operated systems, shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Monitor physical access to the facility where the information is processed or stored to detect and respond to physical security incidents.
   b) Review physical access logs monthly for Low and Moderate categorized information, weekly for High categorized information and in response to a physical security incident.

c) Conduct investigations of apparent security incidents or violations or suspicious physical access activities[5]. Investigation and review results shall be coordinated with the organization's incident response[6] team.
d) Develop and implement remedial actions identified as a result of investigations. A POA&M shall be developed and documented in accordance with POA&M procedures. Refer to Information Security – Security Assessment and Authorization Procedures for POA&M requirements.

PE-6(1) Monitoring Physical Access | Intrusion Alarms / Surveillance Equipment

For Moderate and High Information Systems:

1) SOs, in coordination with OARM, local building management (e.g., Facility, Health and Safety Management Officials), and SIOs, for EPA-operated systems, shall; and SMs, in coordination with IMOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Install and monitor real-time physical intrusion alarms and surveillance equipment.

PE-6(2) Monitoring Physical Access | Automated Intrusion Recognition / Responses

Not selected as part of the control baseline.

PE-6(3) Monitoring Physical Access | Video Surveillance

Not selected as part of the control baseline.

PE-6(4) Monitoring Physical Access | Monitoring Physical Access to Information Systems

For High Information Systems:

1) SOs, in coordination with OARM, local building management (e.g., Facility, Health and Safety Management Officials), and SIOs, for EPA-operated systems, shall; and SMs, in coordination with IMOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Monitor physical access to the information system in addition to the physical access monitoring of the facility.

PE-7 – Visitor Control

Incorporated into PE-2 and PE-3.

PE-8 – Visitor Access Records

For All Information Systems:

1) SOs, in coordination with OARM, local building management (e.g., Facility, Health and Safety Management Officials), and SIOs, for EPA-operated systems, shall; and SMs, in coordination with IMOs, for systems operated on behalf of the EPA, shall ensure service providers:

[5] *Examples of suspicious physical access activities include accesses outside of normal work hours, repeated accesses to areas not normally accessed, accesses for unusual lengths of time and out-of-sequence accesses.*
[6] *Refer to Information Security – Incident Response Procedures for requirements on incident response.*

a) Maintain visitor access records to the facility where the information system resides in accordance with the National Archives and Records Administration (NARA) requirements. Access records shall include the following:
   i) Name(s) and organization(s) of the person(s) visiting.
   ii) Signature(s) of the visitor(s).
   iii) Forms of identification.
   iv) Date(s) of access.
   v) Entry and departure times.
   vi) Purpose(s) of visit(s).
   vii) Name(s) and organization(s) of person(s) visited.
b) Review visitor access records in response to an information or physical security incident.

Note: Visitor access records are not required for publicly accessible areas.

PE-8(1) – Visitor Access Records | Automated Records Maintenance / Review

For High Information Systems:

1) SOs, in coordination with OARM, local building management (e.g., Facility, Health and Safety Management Officials), and SIOs, for EPA-operated systems, shall; and SMs, in coordination with IMOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Employ automated mechanisms to facilitate the maintenance and review of visitor access records.

PE-8(2) – Visitor Access Records | Physical Access Records

Incorporated into PE-2.

PE-9 – Power Equipment and Cabling

For Moderate and High Information Systems:

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 shall avoid duplicating actions already covered.

1) SOs, in coordination with OARM, local building management (e.g., Facility, Health and Safety Management Officials), and SIOs, for EPA-operated systems, shall; and SMs, in coordination with IMOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Protect power equipment and power cabling for the information system from damage and destruction.
   b) Inspect power cabling annually for indications of fraying or other wear.
      i) Inspect hangers and trays that support power cables for stability.
      ii) Document power cabling inspection results in the Agency Information Security Repository, the Agency's tool for managing POA&Ms, and create a POA&M in the repository correcting weaknesses found.
         (1) Refer to Information Security – Security Assessment and Authorization Procedures for POA&M requirements.

PE-9(1) – Power Equipment and Cabling | Redundant Cabling

Not selected as part of the control baseline.

PE-9(2) – Power Equipment and Cabling | Automatic Voltage Controls

Not selected as part of the control baseline.

PE-10 – Emergency Shutoff

Note: This control applies to facilities containing concentrations of information system resources (e.g., data centers, server rooms and mainframe computer rooms).

For Moderate and High Information Systems:

1) SOs, in coordination with OARM, local building management (e.g., Facility, Health and Safety Management Officials), and SIOs, for EPA-operated systems, shall; and SMs, in coordination with IMOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Provide the capability to shut off power to the information system or individual system components in emergency situations.
      i) Coordination shall occur with facilities management personnel, as needed.
   b) Place emergency shutoff switches or devices in locations as defined by applicable standards to facilitate safe and easy access for personnel. Refer to National Fire Protection Association (NFPA) code NFPA 70.[7]
   c) Document emergency shutoff or shutdown operational procedures. The procedure, at a minimum, shall 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.
      v) Recovery procedures from the emergency shutoff.
      vi) Locations of emergency shutoff devices.
   d) Train all necessary personnel on the emergency shutoff procedures.
   e) Protect the emergency power-off capability from accidental or unauthorized activation.

PE-10(1) – Emergency Shutoff | Accidental / Unauthorized Activation

Incorporated into PE-10.

PE-11 – Emergency Power

For Moderate and High Information Systems:

1) SOs, in coordination with OARM, local building management (e.g., Facility, Health and Safety Management Officials), and SIOs, for EPA-operated systems, shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Provide a short-term Uninterruptible Power Supply (UPS) to facilitate an orderly shutdown of the information system or a transition of the information system to long-term alternate power, as applicable, in the event of a primary power source loss.

[7] *See: http://www.nfpa.org/codes-and-standards/document-information-pages?mode=code&code=70*

PE-11(1) – Emergency Power | Long-Term Alternate Power Supply – Minimal Operational Capability

For High Information Systems:

1) SOs, in coordination with OARM, local building management (e.g., Facility, Health and Safety Management Officials), and SIOs, for EPA-operated systems, shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Provide 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 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 shall be able to support the documented availability requirements for the information system.
      iii) The long-term alternate power supply shall be documented in the Contingency Plan for the information system.
         (1) Refer to Information Security – Contingency Planning Procedures[8] for requirements on Contingency Plans.

PE-11(2) – Emergency Power | Long-Term Alternate Power Supply – Self Contained

Not selected as part of the control baseline.

PE-12 – Emergency Lighting

For All Information Systems:

Note: This requirement applies to facilities containing concentrations of information system resources including data centers, server rooms and mainframe computer rooms.

1) SOs, in coordination with OARM, local building management (e.g., Facility, Health and Safety Management Officials), and SIOs, for EPA-operated systems, shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Employ and maintain 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.
   b) Test the automatic emergency lighting systems annually to ensure they are fully operational.
      i) Document automatic emergency lighting systems test results in the Agency Information Security Repository, the Agency's tool for managing POA&Ms, and create a POA&M in the repository.[9]
         (1) Refer to Information Security – Security Assessment and Authorization Procedures for POA&M requirements.

[8] Refer to the latest version of the EPA Information Security –Contingency Planning Procedures

[9] Refer to EPA Xacta POA&M Guide, Version 2.0, June 2, 2015, Sections: 4, Creating a POA&M, page 14; 5, POA&M Fields, page16; and 6, Guidance on POA&M Fields, page 17; and 7, Creating New POA&Ms, page 23 for guidance on creating POA&Ms in Xacta.

PE-12(1) – Emergency Lighting | Essential Missions / Business Functions

Not selected as part of the control baseline.

PE-13 – Fire Protection

For All Information Systems:

Note: This control applies to facilities containing concentrations of information system resources including data centers, server rooms and mainframe computer rooms. Fire suppression and detection devices/systems include, for example, sprinkler systems, handheld fire extinguishers, fixed fire hoses and smoke detectors.

1) SOs, in coordination with OARM, local building management (e.g., Facility, Health and Safety Management Officials), and SIOs, for EPA-operated systems, shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Employ and maintain fire suppression and detection devices or systems for the information system that are supported by an independent energy source.

PE-13(1) – Fire Protection | Detection Devices / Systems

For High Information Systems:

1) SOs, in coordination with OARM, local building management (e.g., Facility, Health and Safety Management Officials), and SIOs, for EPA-operated systems, shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Provide fire detection devices or systems for the information system that activate automatically and notify designated officials and emergency responders including the local fire department in the event of a fire.

PE-13(2) – Fire Protection | Suppression Devices / Systems

For High Information Systems:

Note: Organizations can identify specific personnel, roles, and emergency responders in the event that individuals on the notification list must have appropriate access authorizations and/or clearances, for example, to obtain access to facilities where classified operations are taking place or where there are information systems containing classified information.

1) SOs, in coordination with OARM, local building management (e.g., Facility, Health and Safety Management Officials), and SIOs, for EPA-operated systems, shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Install fire suppression devices or systems for the information system that provide automatic notification of any activation to designated officials and emergency responders including the local fire department.

PE-13(3) – Fire Protection | Automatic Fire Suppression

For Moderate and High Information Systems:

1) SOs, in coordination with OARM, local building management (e.g., Facility, Health and Safety Management Officials), and SIOs, for EPA-operated systems, shall; and SMs,

in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Provide an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.
b) Ensure Contingency Plans[10] account for suppression system impacts on the system components and plan accordingly.

PE-13(4) – Fire Protection | Inspections

Not selected as part of the control baseline.

PE-14 –Temperature and Humidity Controls

For All Information Systems:

1) SOs, in coordination with OARM, local building management (e.g., Facility, Health and Safety Management Officials), and SIOs, for EPA-operated systems, shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Maintain the temperature and humidity levels within the facility where the information system resides within limits as required by the equipment being protected.
      i) Acceptable temperature and humidity levels shall be defined for the information system.
      ii) This requirement applies to facilities containing concentrations of information system resources including data centers, server rooms and mainframe computer rooms.
   b) Monitor continuously in real time the temperature and humidity levels within the facility where the information system resides.

PE-14(1) – Temperature and Humidity Controls | Automatic Controls

Not selected as part of the control baseline.

PE-14(2) – Temperature and Humidity Controls | Monitoring with Alarms / Notifications

Not selected as part of the control baseline.

PE-15 – Water Damage Protection

1) SOs, in coordination with OARM, local building management (e.g., Facility, Health and Safety Management Officials), and SIOs, for EPA-operated systems, shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Have a master shutoff or isolation valve(s) that is accessible, working properly and known to key personnel in order to protect the information system from damage resulting from water leakage.

   Note: This requirement applies to facilities containing concentrations of information system resources including data centers, server rooms and mainframe computer

[10] *Refer to Information Security – Contingency Planning Procedures for requirements on Contingency Plans*

rooms. Isolation valves can be employed in addition to or in lieu of master shutoff valves to shut off water supplies in specific areas of concern.

PE-15(1) – Water Damage Protection | Automation Support

For High Information Systems:

1) SOs, in coordination with OARM, local building management (e.g., Facility, Health and Safety Management Officials), and SIOs, for EPA-operated systems, shall; and SMs, in coordination with IMOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Employ automated mechanisms that detect the presence of water in the vicinity of the information system and alerts designated officials.

Note: Automated mechanisms can include water detection sensors, alarms and notification systems.

PE-16 – Delivery and Removal

For All Information Systems:

1) SOs, in coordination with OARM, local building management (e.g., Facility, Health and Safety Management Officials), and SIOs, for EPA-operated systems, shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Authorize, monitor and control information system components and packages that:
      i) Are delivered to the facility, can modify or monitor system, facility or space security controls, monitor network traffic or enumerate weaknesses; and
      ii) Are removed from the facility.
   b) Maintain records of those items.

Note: Restricting delivery area(s) access and possibly isolating them from the information system and media libraries may be needed to effectively enforce authorizations for entry and exit of information system components.[11]

PE-17 – Alternate Work Site

For Moderate and High Information Systems:

Note: This control supports the contingency planning activities of organizations and the federal telework initiative.

1) SOs, in coordination with OARM, local building management (e.g., Facility, Health and Safety Management Officials), and SIOs, for EPA-operated systems, shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Employ management, operational and technical information system security controls at alternate work sites 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. While commonly distinct from

[11] *Refer to the latest version of the EPA Information Security – Media Protection Procedures for update guidance.*

alternative processing sites, alternate work sites may provide readily available alternate locations as part of contingency operations.

b) Utilize NIST SP 800-34, Contingency Planning Guide for Federal Information Systems as guidance on Federal information system contingency planning for alternate sites.
c) Assess the effectiveness of security controls at alternate work sites, as feasible.
d) Provide a means (e.g., phone numbers) for employees to communicate with information security personnel in case of security incidents or problems.
e) Utilize NIST SP 800-46, Revision 1, Guide to Enterprise Telework and Remote Access Security as guidance for security in telework and remote access.
f) Ensure users adhere to the following with regard to working in a flexiplace[12] environment:
    i) Comply with all requirements of the information system and those in the Rules of Behavior (ROB).
    ii) Provide access to applicable contact information for reporting suspicious activity.
    iii) Use the computer and remote access capabilities provided by the EPA for authorized activities only.
    iv) Protect equipment and media[13] (e.g., digital, non-digital) from damage and unauthorized access.
    v) Utilize NIST SP 800-114 and NIST SP 800-121 as additional security control guidance for telework, remote access and radio frequency communications used in the establishment of wireless personal area networks (WPAN) supporting 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 shall avoid duplicating actions already covered.

For High Information Systems:

1) SOs, in coordination with OARM, local building management (e.g., Facility, Health and Safety Management Officials), and SIOs, for EPA-operated systems, shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
    a) Position information system components within the facility to minimize potential damage from physical and environmental hazards.[14]

PE-18(1) – Location of Information System Components | Facility Site

Not selected as part of the control baseline.

PE-19 – Information Leakage

Not selected as part of the control baseline.

[12] *Refer to the latest version of EPA Flexiplace Policy 3180 for update guidance.*
[13] *Refer to the latest version the Information Security – Media Protection Procedures for updated guidance.*
[14] *Physical and environmental hazards include, for example, flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electromagnetic pulse, electrical interference and electromagnetic radiation.*

PE-19(1) – Information Leakage | National Emissions / Tempest Policies and Procedures

Not selected as part of the control baseline.

PE-20 – Asset Monitoring and Tracking

Not selected as part of the control baseline.

7. ROLES AND RESPONSIBILITIES

Chief Information Officer (CIO), Office of Environmental Information (OEI)

1) The CIO has the following responsibilities with respect to physical and environmental protection:
   a) Establish minimum mandatory risk based technical, operational and management information security control requirements for Agency information and information systems.
   b) Serve as the Risk Executive for Agency's information Risk Executive Function. As such, coordinating with the Risk Executive Group, OARM and local building management (e.g., Facility, Health and Safety Management Officials), Senior Agency Information Security Officer (SAISO), SIOs, IOs, Information Security Officers (ISO), and SOs in governing risks, including physical and environmental protection procedures.
   c) Review, and may grant, a security control implementation waiver[15] for sufficient reasons exercising judgment in the best interests of the Agency.
   d) Collect and review the POA&Ms, including physical and environmental protection POA&Ms, quarterly.
   e) Collect and review summary information from the POA&M and authorization statuses to ensure EPA oversight reporting requirements to OMB and Congress are fulfilled.
   f) Ensure quarterly POA&M reports, including physical and environmental protection POA&Ms, are provided to OMB as required.

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

1) The responsible OARM and local building management (e.g., Facility, Health and Safety Management Officials), have the following responsibilities with respect to physical and environmental protection:
   a) Coordinate with SOs on planning, implementation and needed improvements to physical and environmental controls at facilities.

Senior Agency Information Security Officer (SAISO)

1) The SAISO has the following responsibilities with respect to physical and environmental protection:
   a) Coordinate with OARM personnel for physical security requirements.

[15] *Refer to EPA Information Security – Risk Assessment Procedures for guidance on wavier processing.*

Assistant Administrators (AA), Regional Administrators (RA) and other key officials (e.g., Principal Deputy Assistant Administrators, Deputy Assistant Administrators, Deputy Regional Administrators, Assistant Regional Administrators, and Office Directors)

1) AAs, RAs and other key officials have the following responsibilities with respect to physical and environmental protection:
   a) Coordinate with the EPA's OARM Security Management Division for physical security requirements. AAs, RAs, or as delegated, Deputy Assistant Administrators or Deputy Regional Administrators, who shall designate in writing Information Security Officers.

Senior Information Officials (SIO)

1) SIOs have the following responsibilities with respect to physical and environmental protection:
   a) Facilitate coordination and implementation of required controls with OARM and local senior management, as needed.
   b) Ensure adequate funding is planned and provided to meet requirements.

Information Management Officers (IMO)

1) IMOs have the following responsibilities with respect to physical and environmental protection:
   a) Ensure that programmatic or Regional requirements, as appropriate, are consolidated and coordinated, as needed.
   b) Raise unresolved issues and funding needs to senior management.
   c) Consolidate plans and budgetary requirements to ensure cost-effective, timely and efficient implementation of requirements.

Director of Office of Information Technology Operations (OITO)

1) The Director of OITO has the following responsibilities with respect to physical and environmental protection:
   a) Coordinate with OARM personnel for physical security requirements.

Computer Security Incident Response Capability (CSIRC)

1) CSIRC has the following responsibilities with respect to physical and environmental protection:
   a) Ensure threat and incident information reported, communicated and used to inform the Agency's information technology security risk management awareness and training, privacy and physical security management programs.

Service Managers (SM)

1) SMs have the following responsibilities with respect to physical and environmental protection:
   a) Implement policies, procedures and control techniques identified in the Agency Information Security Plan (AISP).[16]
   b) Coordinate with CSIRC for enterprise services.

[16] *See EPA Office of Environmental Information (OEI), Information Security Program Manual, Section 9, Technical Controls, subsection 9.3, Physical and Environmental Controls.*

c) Ensure procedures, control techniques and other countermeasures as necessary to support and implement agency Information Security Program requirements are developed and implemented for enterprise services.
d) Follow Federal Risk and Authorization Management Program (FedRAMP[17]) requirements.
    i) Obtain authorizations to operate or authorizations to test from the appropriate SIO prior to operational use or testing of any service for enterprise services
        (1) Coordinate with Information System Security Officers (ISSO), ISOs and IOs to assemble security authorization packages.
    ii) Develop, maintain and provide information security documents as required under the EPA Information Security Program for enterprise services.
        (1) Maintain accurately and up to date all system information security information, such as plans of actions and milestones, system security plans and security assessment reports, in the Agency information security information repository.
        (2) Report systems in the Agency information security system inventory tool and maintaining system information accurately and up to date.
e) Coordinate with key information security personnel such as the SOs, IOs, ISSOs, Common Control Providers (CCP), Security Control Assessors (SCA) and other service managers to determine the information system's security control requirements (common, hybrid and core), implementation, assessments and authorization documentation and continuing monitoring activities.
f) Ensure service providers deploy and operate systems according to the security requirements documented in security plans.
g) Ensure systems supporting non-enterprise services are configured, monitored and maintained to adequately protect supported information stored, processed or transmitted within acceptable risks in accordance with the Agency's requirements.
h) Ensure all information security controls are assessed prior to systems becoming operational and at a minimum, one third of the security controls are assessed at least once every year or when significant changes are made after the initial Authority to Operate (ATO) has been obtained and until the system is decommissioned.
i) Ensure defined core controls are assessed annually as part of the subset (one-third) of the security controls required for annual assessments.
j) Ensure control assessments are conducted by independent assessors or assessment teams for moderate and high categorized systems and obtain Security Assessment Reports (SAR) from assessors.
k) Ensure service providers develop and manage POA&Ms for discovered weaknesses for enterprise services.
l) Coordinate with the Agency's ISOs and SOs to enter and manage POA&Ms in the Agency's FISMA reporting and tracking tool.

Information Security Officers (ISO)

1) ISOs have the following responsibilities with respect to physical and environmental protection:

[17] *FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization and continuous monitoring for cloud products and services.*

a) Ensure that programmatic or Regional requirements, as appropriate, are consolidated and coordinated, as needed.
b) Raise unresolved issues and funding needs to senior management.
c) Consolidate plans and budgetary requirements to ensure cost-effective, timely and efficient implementation of requirements.

System Owners (SO)

1) SOs have the following responsibilities with respect to physical and environmental protection:
   a) Comply with Agency policies and procedures for physical and environmental controls pertaining to facilities and to designated areas where information systems and components reside.
   b) Determine specific physical and environmental control requirements for their information systems' facilities and designated areas.
   c) 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.
   d) 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.
   e) Ensure appropriate responsible personnel are assigned to conduct reviews for relevant PE controls for the annual FISMA review and certification requirements.

Information System Security Officers (ISSO)

1) ISSOs have the following responsibilities with respect to physical and environmental protection:
   a) Implement the operational aspects of the SO's responsibilities.
   b) Assist SOs and managers in planning, reviewing and implementing required controls.

Users / Individuals

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

OEI Offices / Facilities[18]

1) Each OEI office and facility has the following responsibilities with respect to physical and environmental protection:
   a) Coordinate to ensure necessary physical security measures and access controls are in place to effect positive security and control over access to information, information systems and workplaces and provide the highest degree of security and safety for employees and visitors.

[18] *EPA Office of Environmental Information (OEI), Information Security Program Manual, Section 9, Technical Controls, subsection 9.3, Physical and Environmental Controls, defines these responsibilities for the OEI office and facility.*

8. RELATED INFORMATION

- NIST Special Publications, 800 series
- Federal Identity, Credential and Access Management (FICAM)

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.
- **Authorization Credentials:** include, for example, badges, identification cards and smart cards. Organizations determine the strength of authorization credentials needed (including level of forge-proof badges, smart cards or identification cards) consistent with Federal standards, policies and procedures.
- **Electronic Data Storage:** storage that 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 (aka: Flexible Workplace or Telecommuting):** refers to paid employment performed away from the office, either at home or at a satellite worksite location, for 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):** to officially document the action or decision, either manually or electronically, and includes a signature.

Abbreviations including acronyms are summarized in *Appendix: Acronyms & Abbreviations*.

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 of OITO shall coordinate to maintain a central repository of all waivers.

11. MATERIAL SUPERSEDED

EPA Information Procedures: CIO-2150.3-P-11.1, Information Security – Interim Physical and Environmental Protection Procedures, May 4, 2012.

12. CONTACTS

For further information, please contact the Office of Environmental Information, Office of Information Security & Privacy (OISP).

Ann Dunkin
Chief Information Officer
U.S. Environmental Protection Agency

Information Security – Interim Physical and Environmental Protection Procedures		
Directive No.: 2150-P-11.2	CIO Approval: 12/30/2016	Transmittal No.: 17-004d

APPENDIX:
ACRONYMS & ABBREVIATIONS

AA	Assistant Administrator
AISP	Agency Information Security Plan
ATO	Authority to Operate
CCP	Common Control Provider
CIO	Chief Information Officer
CSIRC	Computer Security Incident Response Capability
DHS	Department of Homeland Security
DoD	Department of Defense
EPA	Environmental Protection Agency
FedRAMP	Federal Risk and Authorization Management Program
FICAM	Federal Identity, Credential and Access Management
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
FOIA	Freedom of Information Act
GSA	General Services Administration
HSPD	Homeland Security Presidential Directive
IMO	Information Management Officer
IO	Information Owner
ISO	Information Security Officer
ISSO	Information System Security Officer
NARA	National Archives and Records Administration
NFPA	National Fire Protection Association
NIST	National Institute of Standards and Technology
OARM	Office of Administration and Resources Management
OEI	Office of Environmental Information
OISP	Office of Information Security & Privacy
OITO	Office of Information Technology Operations
OMB	Office of Management and Budget
PE	Physical and Environmental Protection
PIV	Personal Identity Verification
POA&M	Plan of Action and Milestones
RA	Regional Administrator
ROB	Rules of Behavior
SAISO	Senior Agency Information Security Officer
SAR	Security Assessment Report
SCA	Security Control Assessor
SIO	Senior Information Official
SM	Service Manager
SO	System Owner
SP	Special Publication
UPS	Uninterruptible Power Supply
USC	United States Code
WPAN	Wireless Personal Area Network