# IT Security Procedural Guide: Physical and Environmental Protection (PE) CIO-IT Security-12-64

**Revision 5**

July 8, 2025

Office of the Chief Information Security Officer

## VERSION HISTORY/CHANGE RECORD

| Change Number | Person Posting Change | Change | Reason for Change | Page Number of Change |
|---|---|---|---|---|
| | | **Revision 1 – March 30, 2012** | | |
| 1 | Heard | New product. | Provide guidance for NIST 800 53 Rev 4 controls. | Various |
| | | **Revision 2 – May 16, 2016** | | |
| 1 | Sitcharing | Changes made throughout the document to reflect NIST and GSA requirements. | Updated to reflect and implement most current NIST 800-53 and GSA requirements. | Various |
| 2 | Klemens/ Wilson | Changes made throughout the document to reflect Government comments. | Updated to reflect Government comments. | Various |
| | | **Revision 3 – May 22, 2018** | | |
| 1 | Feliksa/ Klemens | Updated format and NIST SP 800-53 control parameters, added a section on SCRM, included EO 13800 and NIST Cybersecurity Framework. | Biennial update. | Various |
| | | **Revision 4 - April 20, 2022** | | |
| 1 | Dean/ Klemens | Revisions included:<br>● Updated to NIST SP 800-53, Revision 5 controls, GSA parameters, and implementation statements.<br>● Updated format and content. | Align to current NIST guidance and GSA parameters. New or substantively changed controls from Revision 5 are: PE-1, PE-5, PE-8, PE-8(1), PE-8(3), PE-10, PE-11(1), PE-13(1), PE-13(2), PE-14, PE-15(1), PE-17. | Throughout |
| | | **Revision 5 - July 8, 2025** | | |
| | Peralta/ Normand/ Klemens | Revisions included:<br>● Updated controls to add leading zeros and to align with CTW.<br>● Moved policy, references, and roles and responsibilities to appendices.<br>● Aligned to current guide formatting and style. | Periodic update. | Throughout |

# Approval

IT Security Procedural Guide: Physical and Environmental Protection (PE), CIO-IT Security 12-64, Revision 5, is hereby approved for distribution.

DocuSigned by:

Joseph Hoyt

CA8EF810EDA7425...

Joseph Hoyt
Acting GSA Chief Information Security Officer

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

# Table of Contents

## List of Tables

**Note:** Hyperlinks in running text will be provided if they link to a location within this document or a form (i.e., a different section or an appendix). Hyperlinks for external documents and GSA policies and guides will only be provided in Appendix C.

# 1 Introduction

The General Services Administration (GSA) systems and system components must be protected from physical and environmental (PE) threats. The principles and practices described in this guide are based on guidance from the National Institute of Standards and Technology (NIST) including NIST Special Publication (SP) 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations." This guide provides an overview of GSA roles and responsibilities for implementing PE control requirements, PE control applicability per Federal Information Processing Standards (FIPS) Publication 199, "Standards for Security Categorization of Federal Information and Information Systems" security categorization level, and guidance regarding implementing PE controls and their requirements. Throughout the remainder of this guide the identifier PE will be used when referring to the NIST Physical and Environmental Protection controls or the control family, otherwise physical and environmental will be used.

Every GSA system must follow the practices identified in this guide. Any deviations from the security requirements established in GSA Order Chief Information Officer (CIO) 2100.1, "GSA Information Technology (IT) Security Policy" must be coordinated by the Information Systems Security Officer (ISSO) through the appropriate Information Systems Security Manager (ISSM) and authorized by the Authorizing Official (AO). Any deviations, exceptions, or other conditions not following GSA policies and standards must be submitted using the Security Deviation/Waiver Request Google Form.

Executive Order (EO) 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," requires all agencies to use "The Framework for Improving Critical Infrastructure Cybersecurity (the Framework) developed by NIST or any successor document to manage the agency's cybersecurity risk." The National Institute of Standards and Technology (NIST) has published The NIST Cybersecurity Framework (CSF) 2.0 (CSF 2.0) as the latest version of the Framework. The GSA uses NIST Special Publication (SP) 800-37, Revision 2, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy," commonly referred to as the RMF, as its foundation for managing risk, including the implementation of security and privacy programs identified in NIST SP 800-53 Revision 5, "Security and Privacy Controls for Information Systems and Organizations." Further information on how PE controls relate to the CSF is provided in Appendix A.

## 1.1 Purpose

The purpose of this guide is to provide guidance for the implementation of PE controls in NIST SP 800-53 and physical and environmental requirements specified in CIO 2100.1. This procedural guide provides GSA Federal employees and contractors with significant security responsibilities, as identified in CIO 2100.1, and other IT personnel involved in the physical and environmental protection for IT assets, the specific procedures and processes they are to follow for protecting GSA systems under their purview, including the information stored, processed, or transmitted by those systems. Federal or Vendor/Contractor facilities management offices may be heavily involved in implementing NIST controls and GSA requirements, especially where controls are associated with multiple systems.

## 1.2 Scope

The requirements outlined within this guide apply to and must be followed by all GSA Federal employees and contractors who are involved in providing physical and environmental protection of GSA systems and information. All GSA systems must adhere to the requirements and guidance provided with regard to the procedures, processes, and methods for providing physical and environmental protections as described in this guide. Per CIO 2100.1, a GSA system is a system used or operated:

- by the GSA; or
- on behalf of the GSA by a contractor of the GSA or by another organization.

## 1.3 Policy

Appendix B contains the policy statements regarding physical and environmental protection.

## 1.4 References

Appendix C contains a list of references used throughout this guide.

# 2 Roles and Responsibilities

Appendix D contains the roles and responsibilities associated with physical and environmental protection.

# 3 GSA Implementation Guidance for PE Controls

The GSA-defined parameter settings included in the control requirements are in blue text and offset by brackets in the control text. As stated in Section 1.2, Scope, the requirements outlined within this guide apply to all GSA systems and must be followed by all GSA Federal employees and contractors involved in the physical and environmental protection of GSA information systems and data. The GSA implementation guidance stated for each control applies to personnel and/or the information systems operated on behalf of the GSA. Any additional instructions or requirements for contractor systems will be included in the "Additional Contractor System Considerations" portion of each control section.

Table 3-1 identifies the designation of PE controls as Common, Hybrid, or System-Specific Controls for Federal and Contractor systems. Effectively, common controls are provided by the GSA at the enterprise level or by one of GSA's Major Information Systems (e.g., General Support System), system-specific controls are implemented at the system level, and hybrid controls have shared responsibilities. GSA CIO-IT Security-Privacy-18-90, the Common Control Catalog (CCC), describes the GSA enterprise-wide common and hybrid controls and outlines the responsible parties for implementing them.

**Table 3-1. Designation of PE Controls**

| Control Designation | Federal System | Contractor System |
|---|---|---|
| **Common** | PE-01 | None |
| **Hybrid** | None | None |

| | | |
|---|---|---|
| **System-Specific** | PE-02, PE-03, PE-03(01), PE-04, PE-05, PE-06, PE-06(01), PE-06(04), PE-08, PE-08(01), PE-08(03), PE-09, PE-10, PE-11, PE-11(01), PE-12, PE-13, PE-13(01), PE-13(02), PE-14, PE-15, PE-15(01), PE-16, PE-17, PE-18 | PE-01, PE-02, PE-03, PE-03(01), PE-04, PE-05, PE-06, PE-06(01), PE-06(04), PE-08, PE-08(01), PE-08(03), PE-09, PE-10, PE-11, PE-11(01), PE-12, PE-13, PE-13(01), PE-13(02), PE-14, PE-15, PE-15(01), PE-16, PE-17, PE-18 |

Table 3-2 identifies the PE control applicability at the FIPS 199 Low, Moderate, and High levels.

### Table 3-2. PE Control Applicability

| FIPS 199 Level | Applicable Controls |
|---|---|
| **Low** | PE-01, PE-02, PE-03, PE-06, PE-08, PE-12, PE-13, PE-14, PE-15, PE-16 |
| **Moderate** | PE-01, PE-02, PE-03, PE-04, PE-05, PE-06, PE-06(01), PE-08, PE-08(03)*, PE-09, PE-10, PE-11, PE-12, PE-13, PE-13(1), PE-14, PE-15, PE-16, PE-17 |
| **High** | PE-01, PE-02, PE-03, PE-03(01), PE-04, PE-05, PE-06, PE-06(01), PE-06(04), PE-08, PE-08(01), PE-08(03)*, PE-09, PE-10, PE-11, PE-11(01), PE-12, PE-13(01), PE-13(02), PE-14, PE-15, PE-15(01), PE-16, PE-17, PE-18 |

*-control is applicable at the level listed per GSA OCISO tailoring.

For readers' ease of use, "mini tables" (see Table 3-3) that contain control/enhancement designation and applicability information are provided at the end of control statements for each PE control. The tables allow readers to see if a control/enhancement is applicable at their system's FIPS Level/A&A process and if it is common (C), hybrid (H), or system specific (S), eliminating the need to refer back to Tables 3-1 and 3-2 for this information.

### Table 3-3. Example Mini Table

| | Low | Mod | High | Federal | Contractor |
|---|---|---|---|---|---|
| Control ID | ✓ | ✓ | ✓ | C | H |

## 3.1 PE-01 Policy and Procedures

**Control:**

a. Develop, document, and disseminate to [personnel with IT security responsibilities as defined in GSA CIO Order 2100.1]:
   1. [Organization-level] physical and environmental protection policy that:
      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
   2. Procedures to facilitate the implementation of the physical and environmental protection policy and the associated physical and environmental protection controls;

b. Designate an [CISO] to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures; and

c. Review and update the current physical and environmental protection:
   1. Policy [annually, as part of CIO 2100.1, GSA IT Security Policy] and following [changes to Federal or GSA policies, requirements, or guidance]; and
   2. Procedures [at least every three (3) years] and following [changes to Federal or GSA policies, requirements, or guidance].

| | Low | Mod | High | Federal | Contractor |
|---|---|---|---|---|---|
| PE-01 | ✓ | ✓ | ✓ | C | H |

**Common Control Implementation**
For PE-01,GSA's physical and environmental protection policy is defined in the GSA IT Security Policy, CIO 2100.1, which addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance regarding physical and environmental protection for GSA systems. This policy is maintained to be consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines by updating the policy via Changes, Instructional Letters, or the annual update as applicable. This policy is disseminated GSA-wide via GSA's InSite centralized agency web site.

GSA's physical and environmental protection procedures are documented in GSA CIO-IT Security-12-64: Physical and Environmental Protection (PE). The procedures facilitate the implementation of the physical and environmental protection policy and associated controls. This guide is disseminated GSA-wide via GSA's InSite centralized agency web site.

Per CIO 2100.1, the CISO is responsible for managing the development and publishing of all security policies and IT security procedural guides. The GSA OCISO is responsible for reviewing and updating CIO 2100.1 annually. The GSA OCISO is responsible for reviewing and updating GSA CIO-IT Security-12-64 every three years and following changes to Federal or GSA policies, requirements, or guidance.

**Federal System-Specific Expectation**
None, PE-01 is a common control.

**Vendor/Contractor System-Specific Expectation**
Vendors/Contractors may defer to the GSA policy and guide or implement their own physical and environmental policies and procedures which comply with GSA's requirements with the approval of the Authorizing Official (AO).

## 3.2 PE-02 Physical Access Authorizations

**Control:**

a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides;
b. Issue authorization credentials for facility access;
c. Review the access list detailing authorized facility access by individuals [at least annually]; and
d. Remove individuals from the facility access list when access is no longer required.

| | Low | Mod | High | Federal | Contractor |
|---|---|---|---|---|---|
| PE-02 | ✓ | ✓ | ✓ | S | S |

**System-Specific Guidance**
The GSA requires a current list of personnel and roles authorized physical access to the system to be maintained along with the appropriate System Security and Privacy Plan (SSPP). The GSA requires the acceptance of Federal Personal Identity Verification (PIV) smartcard credentials as the common means to authenticate federal employee and contractor access to

GSA facilities, networks, and information systems. The facility access list has to be updated and reviewed at least annually. Individuals must be removed from the facility access list when they no longer need access based on a change in their duties or termination/transfer as specified in GSA CIO-IT Security-03-23: Termination and Transfer.

This control only applies to areas within facilities that have not been designated as publicly accessible. Due to the sensitive nature of information stored within GSA facilities, it is important that individuals lacking sufficient security clearances, access approvals, or a business 'need-to-know,' be escorted by individuals with appropriate credentials to ensure that such information is not exposed or otherwise compromised.

## 3.3 PE-03 Physical Access Control

**Control:**

a. Enforce physical access authorizations at [GSA SSO or Contractor recommended and GSA CISO and AO approved entry/exit points to the facility where the information system resides] by:
   1. Verifying individual access authorizations before granting access to the facility; and
   2. Controlling ingress and egress to the facility using [Physical Access Control Systems (PACS) devices IAW GSA Order ADM 5900.1, and guards for on-premises contracts; GSA SSO or Contractor recommended and GSA CISO and AO approved physical access control systems, devices, guards for off-premises contracts];
b. Maintain physical access audit logs for [GSA SSO or Contractor recommended entry/exit points approved by the GSA CISO and AO];
c. Control access to areas within the facility designated as publicly accessible by implementing the following controls: [GSA SSO or Contractor recommended physical access controls approved by the GSA CISO and AO];
d. Escort visitors and control visitor activity [GSA SSO or Contractor recommended circumstances requiring visitor escorts and monitoring approved by the GSA CISO and AO];
e. Secure keys, combinations, and other physical access devices;
f. Inventory [GSA SSO or Contractor recommended physical access devices approved by the GSA CISO and AO] every [year]; and
g. Change combinations and keys [at least annually] and/or when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated.

**Control Enhancements:**

(01) Physical Access Control | System Access. Enforce physical access authorizations to the system in addition to the physical access controls for the facility at [GSA SSO or Contractor recommended and GSA CISO and AO approved physical spaces containing one or more components of the information system].

| | Low | Mod | High | Federal | Contractor |
|---|---|---|---|---|---|
| PE-03 | ✓ | ✓ | ✓ | S | S |
| PE-03(01) | | | ✓ | S | S |

**System-Specific Guidance**
For PE-(03), individuals' access authorizations to facilities must be verified (i.e., ensuring they are on the access list) prior to granting access to the facility hosting information systems. The

GSA requires mandatory use of PIV credentials for individual access to GSA facilities. Additionally, the GSA has established an agency-wide approach and policy to update, procure, and install HSPD-12 compliant Physical Access Control Systems (PACS) in GSA controlled space(s) IAW GSA Order ADM 5900.1, “Physical Access Control Systems in U.S. General Services Administration Controlled Space.” Ingress/egress to information systems in non-GSA facilities must be controlled using GSA CISO and AO approved physical access control systems, devices, guards.

Physical access audit logs must be maintained at the GSA facility in which the information system resides and reviewed IAW PE-06. Audit logs can be procedural (e.g., a written log of individuals accessing the GSA facility and when such access occurred), automated (e.g., capturing ID provided by a PIV card), or some combination thereof. Physical access points can include GSA facility access points, interior access points to information systems and/or components requiring supplemental access controls, or both. When escorts are required, the escort must be identified in the visitor access record IAW PE-08.

Keys, combinations, and other physical access devices must be secured (as necessary) and changed at least annually. Inventories of physical access devices must be approved annually by the GSA CISO and AO.

For PE-03(01), systems must control physical access authorizations and restrict access to GSA AO approved physical areas containing the system or any of its components. For example, controlling access to individual cages or racks in addition to the facility controls.

## 3.4 PE-04 Access Control for Transmission

**Control:** Control physical access to [GSA SSO or Contractor recommended and GSA CISO and AO approved information system distribution and transmission lines] within organizational facilities using [GSA SSO or Contractor recommended and GSA CISO and AO approved security controls].

| | Low | Mod | High | Federal | Contractor |
|---|---|---|---|---|---|
| PE-04 | | ✓ | ✓ | S | S |

**System-Specific Guidance**
This control ensures the GSA and its custodians protect against accidental or intentional damage or disruption of distribution and transmission lines located within facilities housing GSA information systems. In addition, physical safeguards may be necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Adequate protections include but are not limited to locked wiring closets, use of protective cable conduit or trays, and disconnecting or locking spare jacks.

## 3.5 PE-05 Access Control for Output Devices

**Control:** Control physical access to output from [all IT assets] to prevent unauthorized individuals from obtaining the output.

| | Low | Mod | High | Federal | Contractor |
|---|---|---|---|---|---|
| PE-05 | | ✓ | ✓ | S | S |

**System-Specific Guidance**

The output of GSA systems must be protected from physical access by unauthorized individuals by controlling the output locations and access to them. Examples of output devices are monitors, printers/facsimile devices/copiers, and audio devices. Protective methods include locating output devices within controlled access areas, separate from areas designated publicly accessible. For devices such as monitors, in addition to controlling the space where they are located, filters/screens can be used to hinder casual observation.

## 3.6 PE-06 Monitoring Physical Access

**Control:**

a. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents;
b. Review physical access logs [at least annually] and upon occurrence of [physical security incidents]; and
c. Coordinate results of reviews and investigations with the organizational incident response capability.

**Control Enhancements:**

(01) Monitoring Physical Access | Intrusion Alarms and Surveillance Equipment. Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment.

(04) Monitoring Physical Access | Monitoring Physical Access to Systems. Monitor physical access to the system in addition to the physical access monitoring of the facility at [GSA SSO or Contractor recommended and GSA CISO and AO approved physical spaces containing one or more components of the information system].

| | Low | Mod | High | Federal | Contractor |
|---|---|---|---|---|---|
| PE-06 | ✓ | ✓ | ✓ | S | S |
| PE-06(01) | | ✓ | ✓ | S | S |
| PE-06(04) | | | ✓ | S | S |

**System-Specific Guidance**

For PE-06, physical access to locations containing one or more components of GSA systems must be monitored to identify and respond to physical intrusions. Examples of monitoring capabilities are guards, cameras, and sensors. If a physical security incident occurs logs must be reviewed as part of the incident investigation and logs must be reviewed at least annually to ensure that they are being maintained and contain required information. Any incidents involving GSA systems must be handled based on the activities in GSA CIO-IT Security-01-02: Incident Response (IR).

For PE-06(01), systems must provide physical intrusion alarms and surveillance equipment within the facility housing the information system or any information system components. Example implementations include motion or contact sensors and video cameras.

For PE-06(04), systems must provide additional monitoring for those areas within facilities where there is a concentration of information system components (e.g., server rooms, media storage areas, communications centers) as approved by the GSA CISO and AO.

## 3.7 PE-08 Visitor Access Records

**Control:**

a. Maintain visitor access records to the facility where the system resides for [at a minimum 2 years per NARA GRS 5.6, Item 111];
b. Review visitor access records [at least annually]; and
c. Report anomalies in visitor access records to [ISSO, ISSM, and facility security staff (e.g., Federal Protective Service)].

**Control Enhancements:**

(01) Visitor Access Records | Automated Records Maintenance and Review. Maintain and review visitor access records using [GSA SSO or Contractor recommended GSA CISO and AO approved automated mechanisms].
(03) Visitor Access Records | Limit Personally Identifiable Information Elements. Limit personally identifiable information contained in visitor access records to the following elements identified in the privacy risk assessment: [individual visitor's name].

| | Privacy | Low | Mod | High | Federal | Contractor |
|---|---|---|---|---|---|---|
| PE-08 | | ✓ | ✓ | ✓ | S | S |
| PE-08(01) | | | | ✓ | S | S |
| PE-08(03) | ✓ | | ✓* | ✓* | S | S |

*Control is applicable per GSA OCISO tailoring.

**System-Specific Guidance**

For PE-08, systems/custodians of systems must maintain visitor access records to facilities where systems reside for at least two years per NARA GRS 5.6, Item 111 or longer if approved by the GSA CISO and AO. Logs must be reviewed at least annually to ensure they are being maintained and contain the required information (see below). Anomalies in visitor access records (e.g., missing data, gaps in records) must be reported to the ISSO, ISSM, and the facility security staff (e.g., Federal Protective Service).

Visitor access records must include the following information:

- Name and Organization of the person visiting;
- Signature of the visitor;
- Form of identification;
- Date of access;
- Time of entry and departure;
- Purpose of visit;
- Name and organization of person visited; and
- Signature and name of individual verifying the visitor’s credentials.

For PE-08(01), systems must implement automated mechanisms to assist in the review of visitor access records. Examples of mechanisms used to support the requirements of this enhancement would be reports generated from physical access control systems and visitor registration systems.

For PE-08(03), systems must limit the personally identifiable information contained in visitor access records to the individual visitor’s name.

## 3.8 PE-09 Power Equipment and Cabling

**Control:** Protect power equipment and power cabling for the system from damage and destruction.

| | Low | Mod | High | Federal | Contractor |
|---|---|---|---|---|---|
| PE-09 | | ✓ | ✓ | S | S |

**System-Specific Guidance**
For PE-09, the GSA Federal and contracted facilities generally satisfy this control requirement through facility design requirements. GSA determines the types of protection necessary for power equipment and cabling employed at different locations both internal and external to organizational facilities and environments of operation. This includes, for example, generators and power cabling outside of buildings, internal cabling and uninterruptible power sources within an office or data center, and power sources.

## 3.9 PE-10 Emergency Shutoff

**Control:**

a. Provide the capability of shutting off power to [any physical equipment] in emergency situations;
b. Place emergency shutoff switches or devices in [GSA SSO or Contractor recommended and GSA CISO and AO approved location by information system or system component] to facilitate access for authorized personnel; and
c. Protect emergency power shutoff capability from unauthorized activation.

| | Low | Mod | High | Federal | Contractor |
|---|---|---|---|---|---|
| PE-10 | | ✓ | ✓ | S | S |

**System-Specific Guidance**
For PE-10, the GSA Federal or contracted facilities must have the ability to shut off power in the event of an emergency in areas with concentrations of information system resources such as server rooms, tape libraries and data centers. The determination regarding the need for emergency shutoff switches and devices must be considered as part of the overall building design requirements.

All personnel should be aware of emergency power shut off locations. Procedures and cautions regarding their use should be documented. Emergency power shutoff capabilities must be protected from unauthorized activation. For example, having a cage or glass barrier protecting it from inadvertent activation supports protecting it from unauthorized activation..

## 3.10 PE-11 Emergency Power

**Control:** Provide an uninterruptible power supply to facilitate [an orderly shutdown of the information system; transition of the information system to long-term alternate power] in the event of a primary power source loss.

**Control Enhancements:**

(01) Emergency Power | Alternate Power Supply – Minimal Operational Capability. Provide an alternate power supply for the system that is activated [automatically] and that can maintain minimally required operational capability in the event of an extended loss of the primary power source

| | Low | Mod | High | Federal | Contractor |
|---|---|---|---|---|---|
| PE-11 | | ✓ | ✓ | S | S |
| PE-11(01) | | | ✓ | S | S |

**System-Specific Guidance**
For PE-11, systems and their facility/environment must provide an uninterruptible power supply (e.g., battery backup) with sufficient power to allow systems to shut down without data loss or transition to an alternate long term power source (e.g., generators).

For PE-11(01), systems must use a secondary commercial power supply or other external power supply that is activated automatically that allows the system to provide its minimally operated capability if there is an extended power loss. For example, backup power generators may provide this capability.

## 3.11 PE-12 Emergency Lighting

**Control:** Employ and maintain automatic emergency lighting for the system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

| | Low | Mod | High | Federal | Contractor |
|---|---|---|---|---|---|
| PE-12 | ✓ | ✓ | ✓ | S | S |

**System-Specific Guidance**
For PE-12, systems and their facility/environment generally can meet this control through building design, existing building codes and regulations, and specifications included in contracts for facilities housing information systems. Each SSPP must describe how its facilities specifically meet this requirement (i.e., describe how emergency lighting functions and that it covers all aspects of the control statement).

## 3.12 PE-13 Fire Protection

**Control:** Employ and maintain fire detection and suppression systems that are supported by an independent energy source.

**Control Enhancements:**

(01) Fire Protection | Detection Systems – Automatic Activation and Notification. Employ fire detection systems that activate automatically and notify [Information System Security Officer, System Owners, Acquisitions/Contracting Officers, Custodians] and [Police and Fire Department] in the event of a fire.

(02) Fire Protection | Suppression Systems – Automatic Activation and Notification.

(a) Employ fire suppression systems that activate automatically and notify [Information System Security Officer, System Owners, Acquisitions/Contracting Officers, Custodians] and [Police and Fire Department]; and

(b) Employ an automatic fire suppression capability when the facility is not staffed on a continuous basis.

| | Low | Mod | High | Federal | Contractor |
|---|---|---|---|---|---|
| PE-13 | ✓ | ✓ | ✓ | S | S |
| PE-13(01) | | ✓ | ✓ | S | S |
| PE-13(02) | | | ✓ | S | S |

**System-Specific Guidance**
For PE-13, all systems must ensure facilities containing concentrations of information system resources employ and maintain fire suppression and detection devices/systems for the resource(s) and are supported by an independent energy source. This control may be satisfied by building design and existing codes and regulations.

For PE-13(01), fire detection devices/systems must activate automatically and there must be a process defined to notify the personnel/organizations identified in the parameter.

For PE-13(02), fire suppression devices/systems must activate automatically and there must be a process defined to notify the personnel/organizations identified in the parameter. If the facility is not staffed on a continuous basis the fire suppression system must automatically be deployed.

## 3.13 PE-14 Environmental Controls

**Control:**

a. Maintain [temperature; humidity] levels within the facility where the system resides at [Data center temperature range (taken at the server inlets) should be 18 degrees Celsius to 27 degrees (64.4 degrees Fahrenheit to 80.6 degrees). Data center humidity levels (measured by dew point) should be within 5.5 degrees Celsius to 15 degrees (41.9 degrees Fahrenheit to 59 degrees). Ranges are consistent with American Society of Heating, Refrigerating and Air-conditioning Engineers (ASHRAE) guidelines]; and
b. Monitor environmental control levels [continuously].

| | Low | Mod | High | Federal | Contractor |
|---|---|---|---|---|---|
| PE-14 | ✓ | ✓ | ✓ | S | S |

**System-Specific Guidance**
For PE-14, facilities must protect information systems against damage or disruption caused by extreme temperatures or humidity levels. Facility temperature and humidity levels must be consistent with ASHRAE guidelines: temperature for data centers (taken at the server inlets) between 18 - 27° C (64.4 – 80.6° F) and humidity levels, measured by dew point, between 5.5 - 15° C (41.9 - 59° F). The system must document in the SSPP how these levels are maintained and monitored.

## 3.14 PE-15 Water Damage Protection

**Control:** Protect the system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

**Control Enhancements:**

(01) Water Damage Protection | Automation Support. Detect the presence of water near the system and alert [System Owners, and Custodians] using [GSA SSO or Contractor recommended and GSA CISO and AO approved automated mechanisms].

| | Low | Mod | High | Federal | Contractor |
|---|---|---|---|---|---|
| PE-15 | ✓ | ✓ | ✓ | S | S |
| PE-15(01) | | | ✓ | S | S |

**System-Specific Guidance**
For PE-15, all systems must ensure facilities containing concentrations of information system resources employ and maintain water protection capabilities such as master shutoff valves and/or isolation valves that shut off water to zones or areas in the facility which would not affect other zones or areas. Key personnel (e.g., facility managers, personnel monitoring the facility) must know the location for any shut off valves and how to activate them. Data centers and server rooms generally should meet this control based on the specific facility/room design meeting building design codes and regulations.

For PE-15(01), water damage protection systems (i.e., water detection sensors, alarms, and notification systems) must be automated.

## 3.15 PE-16 Delivery and Removal

**Control:**

a. Authorize and control [all information system components] entering and exiting the facility; and
b. Maintain records of the system components

| | Low | Mod | High | Federal | Contractor |
|---|---|---|---|---|---|
| PE-16 | ✓ | ✓ | ✓ | S | S |

**System-Specific Guidance**
For PE-16, controlling and authorizing the delivery and removal of system components supports configuration management, supply chain risk management, and access control from a physical standpoint. All systems must control and manage areas such as delivery docks, staging areas, and any other areas where system components may be delivered or removed. Records of deliveries and removals must be maintained in sufficient detail to know when and what was delivered or removed and who delivered/removed the component and who accepted delivery or authorized removal. A list of authorized personnel, their role, and what they can accept or remove should be maintained.

## 3.16 PE-17 Alternate Work Site

**Control:**

a. Determine and document the [GSA SSO or Contractor defined and GSA CISO and AO approved alternate work sites] allowed for use by employees;

b. Employ the following controls at alternate work sites: [controls as specified in GSA Orders ADM 2450.1, HRM 6040.1 and CIO 2100.1, and other organizations' alternate work site and security policies as approved by the CISO and AO];
c. Assess the effectiveness of controls at alternate work sites; and
d. Provide a means for employees to communicate with information security and privacy personnel in case of incidents

| | Low | Mod | High | Federal | Contractor |
|---|---|---|---|---|---|
| PE-17 | | ✓ | ✓ | S | S |

**System-Specific Guidance**
For PE-17, alternate work sites are sites that are geographically distinct from primary work sites, which must be approved by the GSA CISO and AO for employee use. Alternate work sites may include government facilities (e.g., continuity or disaster recovery locations) or employee residences. Implement control requirements for alternate work sites per the directives listed below and the GSA Telework InSite page (for GSA employees and support contractors).

- GSA Order HRM 6040.1, "GSA Telework Policy"
- GSA Order CIO 2100.1, "GSA Information Technology (IT) Security Policy"

## 3.17 PE-18 Location of System Components

**Control:** Position system components within the facility to minimize potential damage from [GSA SSO or Contractor recommended and GSA CISO and AO approved physical and environmental hazards] and to minimize the opportunity for unauthorized access.

| | Low | Mod | High | Federal | Contractor |
|---|---|---|---|---|---|
| PE-18 | | | ✓ | S | S |

**System-Specific Guidance**
For PE-18, the location of components within the facility with respect to public areas, entry and exit points, and the facility exterior, must be considered to determine how those locations may affect the ability of unauthorized personnel to capture communications traffic, visually or acoustically record information about the system and use it to gain access to the system or information it uses, processes, or transmits. Typically, the geographic location and design of the facility provides protection against physical and environmental hazards such as floods, fires, tornadoes, other acts of nature, and electronic interference or attacks.

## Appendix A: CSF Categories/Subcategories

The CSF provides guidance to organizations to manage cybersecurity risks. Its use can help organizations to better understand, assess, prioritize, and communicate its cybersecurity efforts. The core of the CSF consists of six concurrent and continuous or readily responsive Functions:

- **Govern (GV):** The organization’s cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.
- **Identify (ID):** The organization’s current cybersecurity risks are understood.
- **Protect (PR):** Safeguards to manage the organization’s cybersecurity risks are used.
- **Detect (DE):** Possible cybersecurity attacks and compromises are found and analyzed.
- **Respond (RS):** Actions regarding a detected cybersecurity incident are taken.
- **Recover (RC):** Assets and operations affected by a cybersecurity incident are restored.

The GSA uses the CSF to complement its risk management process and cybersecurity program. The GSA uses NIST’s Risk Management Framework (RMF) from NIST SP 800-37, Revision 2, “Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy” as its foundation for managing system risk. More detailed information on how the CSF relates to GSA’s use of the NIST RMF is contained in GSA CIO-IT Security-06-30: Managing Enterprise Cybersecurity Risk.

Table A-1 lists the Categories and Subcategories from the CSF that are identified as related to the implementation of policies, procedures, and processes regarding the NIST SP 800-53 controls documented in this guide.

### Table A-1. CSF Categories/Subcategories and the PE Control Family

| CSF Category | Subcategory Identifier/Description |
|---|---|
| **Organizational Context (GV.OC):** The circumstances - mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements - surrounding the organization's cybersecurity risk management decisions are understood | **GV.OC-03**: Legal, regulatory, and contractual requirements regarding cybersecurity - including privacy and civil liberties obligations - are understood and managed (PE-03, PE-06) |
| **Policy (GV.PO):** Organizational cybersecurity policy is established, communicated, and enforced | **GV.PO-01:** Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced (PE-01)<br>**GV.PO-02:** Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission (PE-01) |
| **Oversight (GV.OV):** Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy | **GV.OV-01:** Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction (PE-01) |
| **Cybersecurity Supply Chain Risk Management (GV.SC):** Cyber supply chain risk management processes are | **GV.SC-03:** Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes (PE-01) |

| | |
|---|---|
| identified, established, managed, monitored, and improved by organizational stakeholders | |
| **Improvement (ID.IM):** Improvements to organizational cybersecurity risk management processes, procedures and activities are identified across all CSF Functions | **ID.IM-01:** Improvements are identified from evaluations (PE-01)<br>**ID.IM-02:** Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties (PE-01)<br>**ID.IM-03:** Improvements are identified from execution of operational processes, procedures, and activities (PE-01) |
| **Identity Management, Authentication, and Access Control (PR.AA):** Access to physical and logical assets is limited to authorized users, services, and hardware and  managed commensurate with the assessed risk of unauthorized access | **PR.AA-06:** Physical access to assets is managed, monitored, and enforced commensurate with risk (PE-02, PE-03, PE-04, PE-05, PE-06, PE-08, PE-18) |
| **Technology Infrastructure Resilience (PR.IR):** Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, availability, and organizational resilience | **PR.IR-02:** The organization's technology assets are protected from environmental threats ( PE-09, PE-10, PE-11, PE-12, PE-13, PE-14, PE-15, PE-18) |
| **Continuous Monitoring (DE.CM):** Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events | **DE.CM-02**: The physical environment is monitored to find potentially adverse events (PE-03, PE-06) |

## Appendix B: GSA CIO 2100.1 Policy Statements Regarding Physical and Environmental Protection

### Chapter 4, Policy for Protect Function

1. Identity Management, Authentication and Access Control.

n. Physical access to GSA assets must be managed and protected IAW GSA CIOIT Security-12-64: Physical and Environmental Protection (PE). Facilities management offices may be heavily involved in implementing these controls, especially where controls are associated with multiple systems.

o. Physical and environmental security controls must be commensurate with the level of risk and must be sufficient to safeguard IT resources against possible loss, theft, destruction, accidental damage, hazardous conditions, fire, malicious actions, and natural disasters.

p. GSA servers, routers, and other communication hardware essential for maintaining the operability of GSA systems and their connectivity to the GSA Network, must be placed in an isolated, controlled-access location (i.e., behind locked doors).

q. Access to rooms, work areas/spaces, and facilities containing agency systems, networks, and data must be limited to authorized personnel. A list of current personnel with authorized access shall be maintained and reviewed annually to verify the need for continued access and authorization credentials.

r. Visitor access records shall be maintained for facilities containing information systems (except for those areas within the facility officially designated as publicly accessible). These records must be reviewed at least annually. Visitor access records include: (1) Name and organization of the person visiting; (2) Signature of the visitor; (3) Form of identification; (4) Date of access; (5) Time of entry and departure; (6) Purpose of visit; (7) Name and organization of person visited; and (8) Signature and name of the individual verifying the visitor's credentials.

5. Information Protection Processes and Procedures.

j. Ensure that all agency systems and networks are located in areas not in danger of water damage due to leakage from building plumbing lines, shut-off valves, and other similar equipment to support meeting federal and local building codes.

k. Install and ensure operability of fire suppression devices, such as fire extinguishers and sprinkler systems, and detection devices, such as smoke and water detectors, in all areas where agency information systems are maintained (this includes server rooms, tape libraries, and data centers) to meet federal and local building codes.

l. Install and ensure operability of air control devices, such as air-conditioners and humidity controls, in all areas where agency information systems are maintained (this includes server rooms, tape libraries, and data centers) to meet federal and local building codes.

m. The guidance provided in GSA CIO-IT Security-12-64 for a secure physical environment for information systems must be applied. Facilities management offices may be heavily involved in implementing these controls, especially where controls are associated with multiple systems.

## Appendix C: References

**Federal Laws, Standards, Regulations, and Publications:**

- EO 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
- FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems
- HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors
- General Records Schedule (GRS) 5.6, National Archives and Records Administration (NARA)
- NIST Cybersecurity Framework (CSF) 2.0, Framework for Improving Critical Infrastructure Cybersecurity
- NIST SP 800-37, Revision 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
- NIST SP 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations

**GSA Policies, Procedures, Guidance:**

The GSA policies listed below are available on the GSA.gov Directives Library page.

- GSA Order ADM 5900.1, Physical Access Control Systems (PACS) in GSA-Controlled Space
- GSA Order HRM 6040.1, GSA Telework Policy
- GSA Order CIO 2100.1, GSA Information Technology (IT) Security Policy

The GSA CIO-IT Security Procedural Guides listed below are available on the GSA.gov IT Security Procedural Guides page with the exception of GSA CIO-IT Security 09-44 and GSA CIO-IT Security-Privacy-18-90 and which are restricted. These are available on the internal GSA InSite IT Security Procedural Guides page.

- GSA CIO-IT Security-01-02: Incident Response (IR)
- GSA CIO-IT Security-03-23: Termination and Transfer
- GSA CIO-IT Security-06-30: Managing Enterprise Cybersecurity Risk
- GSA CIO-IT Security-09-44: Plan of Action and Milestones (POA&M)
- GSA CIO-IT Security-Privacy-18-90: Common Control Catalog (CCC)

# Appendix D: Roles and Responsibilities

There are many roles associated with implementing effective physical and environmental protection policies and procedures. The roles and responsibilities provided in this section have been extracted or paraphrased from CIO 2100.1 or summarized from GSA and Federal guidance. The responsibilities listed in this guide are focused on physical and environmental protection, a complete set of GSA security roles and responsibilities can be found in CIO 2100.1. Throughout this guide, specific processes, and procedures for implementing NIST SP 800-53 PE controls are described.

## Authorizing Official (AO)

Responsibilities include the following:

- Ensuring that GSA information systems under their purview have implemented the required NIST SP 800-53 PE controls in accordance with GSA and Federal policies and requirements.
- Identifying the level of acceptable risk for an information system and determining whether an acceptable level of risk has been obtained, including risks associated with NIST SP 800-53 PE controls.
- Ensuring all information systems, applications, or sets of common controls under their purview have a current Authorization to Operate (ATO) issued per GSA CIO-IT Security-06-30: Managing Enterprise Cybersecurity Risk.
- Ensuring a plan of action and milestones (POA&M) entry is developed and managed to address any NIST SP 800-53 PE controls that are not fully implemented.

## Information Systems Security Manager (ISSM)

Responsibilities include the following:

- Assisting ISSOs, as necessary, to ensure NIST SP 800-53 PE controls are in place and operating as intended.
- Verifying systems under their purview have appropriately addressed NIST SP 800-53 PE controls.
- Coordinating with the AO, System Owner, ISSOs, and OCISO Directors, as necessary, regarding NIST SP 800-53 PE control implementation and compliance with NIST and GSA requirements.
- Working with the ISSO and System Owner to develop and manage POA&Ms identifying NIST SP 800-53 PE controls that are not fully implemented for their respective systems per GSA CIO-IT Security-09-44: Plan of Action and Milestones.

## Information Systems Security Officer (ISSO)

Responsibilities include the following:

- Ensuring necessary NIST SP 800-53 PE controls are in place and operating as intended.
- Coordinating with ISSMs and System Owners, as necessary, identifying NIST SP 800-53 PE control implementation and compliance with NIST and GSA requirements.
- Working with the System Owner and ISSM to develop and manage POA&Ms regarding NIST SP 800-53 PE controls that are not fully implemented for their respective systems per GSA CIO-IT Security-09-44: Plan of Action and Milestones.

### System Owners

Responsibilities include the following:

- Ensuring necessary NIST SP 800-53 PE security controls are in place and operating as intended.
- Coordinating with ISSOs and ISSMs, as necessary, regarding NIST SP 800-53 PE control implementation and compliance with NIST and GSA requirements.
- Working with ISSOs and ISSMs to develop and manage POA&Ms regarding NIST SP 800-53 PE controls that are not fully implemented for their respective systems per GSA CIO-IT Security-09-44: Plan of Action and Milestones.
- Obtaining the resources necessary to securely implement and manage NIST SP 800-53 PE controls for their respective systems.

### Data Owners

Responsibilities include the following:

- Coordinating with System Owners, ISSMs, ISSOs, and Custodians to ensure data is properly stored, maintained, and protected per GSA policies, regulations and any additional guidelines established by GSA.
- Coordinating with IT security personnel including the ISSM and ISSO and System Owners to ensure implementation of NIST SP 800-53 PE controls in compliance with NIST and GSA requirements.

### Custodians

Responsibilities include the following:

- Coordinating with System Owners, ISSMs, ISSOs, to ensure data is properly stored, maintained, and protected per GSA policies, regulations and any additional guidelines established by GSA.

### Authorized Users of IT Resources

Responsibilities include the following:

- Familiarizing themselves with any special requirements for accessing, protecting, and using data, including Privacy Act requirements, copyright requirements, and procurement-sensitive data.
- Ensuring that adequate protection is maintained on their workstation, including not sharing passwords with any other person and logging out, locking, or enabling a password protected screen saver before leaving their workstation.

### Supervisors

Responsibilities include the following:

- Coordinating and arranging system access requests for all new or transferring employees and for verifying an individual’s business ‘need-to-know’ (authorization).
- Coordinating and arranging system access termination for all departing or resigning personnel.
- Coordinating and arranging system access modifications for personnel.