Information Technology (IT) Physical and Environmental Protection (PE) Standard

January 26, 2024

U.S. Department of Education (ED)

Office of the Chief Information Officer (OCIO)

Information Assurance Services (IAS)

Questions about the policies outlined in this document should be directed to Information Assurance Services (IAS) at **IAS_Governance@ed.gov**.

APPROVAL

STEVEN HERNANDEZ

Digitally signed by STEVEN HERNANDEZ
Date: 2024.01.26 17:04:50 -05'00'

Steven Hernandez

Director, IAS/Chief Information Security Officer (CISO)

Revision History

The table below identifies all changes that have been incorporated into this document.

Version	Date	Summary of Changes
1.0	12/22/2021	Initial draft of new standard which combines NIST SP 800-53, Revision 5 controls, including ED specific control parameter values, with existing policy standards.
1.1	1/14/2022	Update to incorporate feedback from Information Assurance Services (IAS), Governance, Risk and Policy (GRP) Team.
1.2	1/31/2022	Update to incorporate feedback from IAS; address new security measures required by Executive Order (EO) 14028, including Office of Management and Budget (OMB) regulations and memoranda and updated NIST guidance issued to comply with the EO.
1.3	1/31/2023	Annual review, update broken links and add footnote to HVA control reference in Section 2.
5.4	01/26/2024	Aligned document major version number to align with NIST SP 800-53 revision number. Clean up formatting and numbering throughout and update broken links. Section 2, Standards was updated to include the description of incorporating organizationally defined parameters (ODP) for controls that may be necessary from external control overlays (e.g., High Value Assets [HVA]). Inserted references to NIST SP 800-53B tailoring guidance. Updated Section 4, Acronyms as appropriate. Updated language in controls PE-01 and PE-17. Added controls PE-03(02) and PE-14(02). Added “leading zeros” to control identifiers in alignment with patch release of NIST SP 800-53 (Release 5.1.1) to applicable controls, enhancements, and overlays.

Table of Contents

1 INTRODUCTION 1
1.1 Purpose 1
1.2 Scope 1
2 STANDARDS 2
2.1 PE-01 Policy and Procedures (L, M, H) 3
2.2 PE-02 Physical Access Authorizations (L, M, H) 4
2.3 PE-03 Physical Access Control (L, M, H) 4
2.4 PE-04 Access Control for Transmission (M, H) 5
2.5 PE-05 Access Control for Output Devices (M, H) 5
2.6 PE-06 Monitoring Physical Access (L, M, H) 5
2.7 PE-08 Visitor Access Records (L, M, H) 6
2.8 PE-09 Power Equipment and Cabling (M, H) 6
2.9 PE-10 Emergency Shutoff (M, H) 6
2.10 PE-11 Emergency Power (M, H) 6
2.11 PE-12 Emergency Lighting (L, M, H) 7
2.12 PE-13 Fire Protection (L, M, H) 7
2.13 PE-14 Environmental Controls (L, M, H) 7
2.14 PE-15 Water Damage Protection (L, M, H) 8
2.15 PE-16 Delivery and Removal (L, M, H) 8
2.16 PE-17 Alternate Work Site (M, H) 8
2.17 PE-18 Location of System Components (H) 8
3 RISK ACCEPTANCE/POLICY EXCEPTIONS 9
4 ACRONYMS 10
APPENDIX A: BASELINE CONTROL PARAMETER SUMMARY 12

1 INTRODUCTION

This governance document establishes Department information technology (IT) system physical and environmental protection standards necessary to improve the efficiency of operation or security of Department information systems and comply with Federal laws, regulations, Executive Orders, Emergency Orders (EO), Binding Operational Directives (BOD), and Department Administrative Communications System Directives (ACSD) and Handbooks. In doing so, these standards supersede any prior governance documentation establishing such standards.

1.1 Purpose

The Federal Information Security Modernization Act (FISMA)[1] and implementing governance Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*[2], requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, and services that are either fully or partially provided, including agency-hosted, outsourced, and cloud-based solutions. Federal Information Processing Standards (FIPS) Publication (PUB) 200, *Minimum Security Requirements for Federal Information and Information Systems*[3], mandates the use of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Information Systems and Organizations*[4], as baseline information system controls.

1.2 Scope

These standards apply to all information and information systems that support the operations and assets of the Department, including those provided or managed by another agency, contractor, or other source, as well as services that are either fully or partially provided, including Department-hosted, outsourced, and cloud-based solutions. Principal Offices, employees, contractors, external service providers and system users are required to comply with these physical and environmental protection control standards.

[1] Public Law 113-283-Dec. 18, 2014, https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf
[2] Office of Management and Budget (OMB) Circular A-130, https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf
[3] FIPS 200, https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.200.pdf
[4] NIST SP 800-53, https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

2 STANDARDS

The Department standards for IT system audit and accountability controls are organized to follow the order in which controls are presented in the current version of NIST SP 800-53. To define a control baseline for Department information systems, a FIPS PUB 199 categorization level (e.g., Low [L], Moderate [M] and High [H]) is assigned to each requirement. This designator indicates a requirement applies to information systems categorized at that FIPS PUB 199 impact-level. Designators are also used to indicate when NIST SP 800-53 Privacy (P) baseline controls are required. To manage risk to within the Department's risk tolerance and appetite, control overlays are provided when the Department requires implementation of control(s) that are not required by the FIPS PUB 199 impact-level or privacy baseline.

In addition to the controls required by this standard, High Value Assets (HVAs) must implement and comply with the current version of the HVA Control Overlay issued and maintained by the Department of Homeland Security (DHS), Cybersecurity & Infrastructure Security Agency (CISA). Systems that process federal tax information (FTI) must implement and comply with the Internal Revenue Service (IRS) Publication 1075[5], *Tax Information Security Guidelines for Federal, State and Local Agencies: Safeguards for Protecting Federal Tax Returns and Return Information.* Systems that are Federal Risk and Authorization Management Program (FedRAMP) authorized must implement and comply with the FedRAMP identified baselines[6].

Throughout the standard, there are controls captured that have not been scoped to any specific security or privacy baseline. This is intentional as all controls for identified external overlays and baselines (e.g., FedRAMP, IRS, HVA), that may apply to systems within the Department, have been incorporated into the standard. This ensures the organization defined parameters (ODPs) for controls within the Department have been clearly defined in a consistent manner.

Based upon an assessment of risk and determination that the level of protection for the security-relevant information within a system is not adversely impacted, maintenance controls identified in the current version of NIST SP 800-53B that support only the availability or confidentiality security objective may be downgraded to the corresponding maintenance control in a lower baseline (or modified or eliminated if not defined in a lower baseline).

This standard directly supports the Department's integration of the NIST Cybersecurity Framework (CSF) and NIST Privacy Framework (PF) by using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the Department's risk management processes. Refer to *APPENDIX A: BASELINE CONTROL PARAMETER SUMMARY* for a summary of controls by baseline and corresponding NIST CSF and NIST PF categories and subcategories.

[5] IRS Publication 1075 https://www.irs.gov/pub/irs-pdf/p1075.pdf
[6] FedRAMP baselines https://www.fedramp.gov/baselines/

2.1 PE-01 Policy and Procedures (L, M, H)

The Department shall develop, document, and disseminate to all ED employees, contractors, and users authorized to access to ED information systems, or systems operated or maintained on behalf of ED, or ED information as defined in ACSD-OCIO-004[7], *Cybersecurity Policy* a Department-level physical and environmental protection policy, ACSD-OFO-031[8], *Physical Security Program*, in addition to this document 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.

c. authorizes the Department Chief Information Security Officer (CISO) and Department Chief Information Officer (CIO) to issue subordinate standards, procedures, and memos, with the same authority and enforcement as ACSD-OCIO-004, *Cybersecurity Policy*.

The Deputy Assistant Secretary, Office of Security, Facilities, and Logistics within the Office of Finance and Operations (OFO) is designated to manage the development, documentation, and dissemination of the Department-level physical security policy. The Department CISO in conjunction with the Senior Agency Official for Privacy (SAOP) and Physical Security Officer are designated to manage the development, documentation, and dissemination of the Department-level IT system physical and environmental protection policy standard (this document).

This policy standard shall be reviewed and updated annually (i.e., each fiscal year) and following the identification of evolving threats, issuance of new or significantly changed existing Federal laws, executive orders, directives, regulations, and ED policies, identification of emerging technology and information technology service delivery models and determination that adjustments are deemed necessary to improve its effectiveness based upon feedback from Principal Office personnel.

Principal Office Information System Owners (ISO) and Information System Security Officers (ISSOs) are required to manage the development, documentation, and dissemination of system specific procedures to facilitate the implementation of the Department's IT system physical and environmental protection policy and the associated physical and environmental protection controls. The ISO and ISSO shall review IT system physical and environmental protection procedures annually (i.e., each fiscal year) and following the identification of evolving threats, issuance of new or significantly changed existing Federal laws, executive orders, directives, regulations, and ED policies, identification of emerging technology and information technology service delivery models and determination that adjustments are deemed necessary to improve its effectiveness based upon feedback from Principal Office personnel.

[7] Also known as OCIO: 3-112.

[8] Also known as OM: 4-114.

2.2 PE-02 Physical Access Authorizations (L, M, H)

Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides. Issue authorization credentials for facility access. Review the access list detailing authorized facility access by individuals at least annually (i.e., each fiscal year) and remove individuals from the facility access list when access is no longer required.

2.3 PE-03 Physical Access Control (L, M, H)

a. Enforce physical access authorizations at designated entry/exit facility access points and interior access points to the system and components by:
    1. Verifying individual access authorizations before granting access to the facility; and
    2. Controlling ingress and egress to the facility using physical access devices such as keys, locks, combinations, biometric readers, card readers, devices and/or guards based upon an assessment of risk.
b. Maintain physical access audit logs for all facility entry/exit points;
c. Control access to areas within the facility designated as publicly accessible by implementing risk appropriate security safeguards;
d. Escort visitors and control visitor activity for individuals requiring visitor escorts and monitoring in non-public areas;
e. Secure keys, combinations, and other physical access devices;
f. Inventory all physical access devices at least annually (i.e., each fiscal year); and
g. Change combinations and keys at least annually (i.e., each fiscal year) and/or when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated.

2.3.1 PE-03(01) Physical Access Control | System Access (H)

Enforce physical access authorizations to the system in addition to the physical access controls for the facility at designated entry/exit facility access points and interior access points to the system and components.

2.3.2 PE-03(02) Physical Access Control | Facility and Systems

Perform security checks at least daily at the physical perimeter of the facility or system for exfiltration of information or removal of system components.

2.4 PE-04 Access Control for Transmission (M, H)[9]

Control physical access to system distribution and transmission lines to include network circuits from the areas within the facility designated for housing the system components within organizational facilities using physical security safeguards to include but not limited to locked wiring closets; disconnected or locked spare jacks; and/or protection of cabling by conduit or cable trays.

2.5 PE-05 Access Control for Output Devices (M, H)[9]

Control physical access to output from devices (e.g., monitors, printers, scanners, audio devices, facsimile machines, copiers, etc.) connected to information systems processing sensitive information to prevent unauthorized individuals from obtaining the output.

2.6 PE-06 Monitoring Physical Access (L, M, H)

a. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents;

b. Review physical access logs as needed and upon occurrence of events or potential indications of events including, but not limited to, suspicious physical activities such as excessive access outside of normal work hours, repeated access to areas not normally accessed, out of sequence access; and

c. Coordinate results of reviews and investigations with the organizational incident response capability.

2.6.1 PE-06(01) Monitoring Physical Access | Intrusion Alarms and Surveillance Equipment (M, H)

Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment.

2.6.2 PE-06(04) Monitoring Physical Access | Monitoring Physical Access to Systems (H)

Monitor physical access to the system in addition to the physical access monitoring of the facility at facilities that contain concentrations of system resources, including data centers, mainframe computer rooms, and server rooms and media storage areas.

[9] PE-04 and PE-05 have been identified by NIST SP 800-53B as supporting only confidentiality and may be downgraded to the corresponding control in a lower baseline (or modified or eliminated if defined in a lower baseline) only if the downgrading action reflects the security category for the supported availability security objective defined impact level.

2.7 PE-08 Visitor Access Records (L, M, H)

a. Maintain visitor access records to the facility where the system resides for at least three (3) years;

b. Review visitor access records on an as needed basis; and

c. Report anomalies in visitor access records to facility security staff, ISO and ISSO.

2.7.1 PE-08(01) Visitor Access Records | Automated Records Maintenance and Review (H)

Maintain and review visitor access records using available, ED approved automated mechanisms such as database management systems which are accessible by Department personnel.

2.7.2 PE-08(03) Visitor Access Records | Limit Personally Identifiable Information Elements (P)

Limit personally identifiable information contained in visitor access records to the following elements identified in the privacy risk assessment: visitor first and last name, organization, purpose of visit, dates/times of visit, as well as first and last name of facility escort.

2.8 PE-09 Power Equipment and Cabling (M, H)[10]

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

2.9 PE-10 Emergency Shutoff (M, H)[10]

a. Provide the capability of shutting off power to information systems or individual system components in emergency situations;

b. Place emergency shutoff switches or devices in facilities that contain concentrations of system resources, including data centers, mainframe computer rooms, and server rooms) to facilitate access for authorized personnel; and

c. Protect emergency power shutoff capability from unauthorized activation.

2.10 PE-11 Emergency Power (M, H)[10]

Provide an uninterruptible power supply to facilitate an orderly shutdown of the information system and/or transition of the information system to long-term alternate power in the event of a primary power source loss.

[10] PE-09, PE-10, and PE-11 have been identified by NIST SP 800-53B as supporting only availability and may be downgraded to the corresponding control in a lower baseline (or modified or eliminated if defined in a lower baseline) only if the downgrading action reflects the security category for the supported availability security objective defined impact level.

2.10.1 PE-11(01) Emergency Power | Alternate Power Supply – Minimal Operational Capability (H)[11]

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.

2.11 PE-12 Emergency Lighting (L, M, H)

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.

2.12 PE-13 Fire Protection (L, M, H)

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

2.12.1 PE-13(01) Fire Protection | Detection Systems – Automatic Activation and Notification (M, H)[11]

Employ fire detection systems that activate automatically and notify facility personnel or roles with facility management and/or physical security responsibilities and emergency responders (e.g., Police and Fire Department) in the event of a fire.

2.12.2 PE-13(02) Fire Protection | Suppression Systems – Automatic Activation and Notification (H)[11]

a. Employ fire suppression systems that activate automatically and notify facility personnel or roles with facility management and/or physical security responsibilities and emergency responders (e.g., Police and Fire Department); and

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

2.13 PE-14 Environmental Controls (L, M, H)

a. Maintain temperature and humidity levels within the facility where the system resides at acceptable levels which ensure systems and equipment operate within vendor recommended limits, if any, and ranges consistent with American Society of Heating, Refrigerating and Air-conditioning Engineers (ASHRAE) guidelines for temperature and humidity; and

[11] PE-11(01), PE-13(01) and PE-13(02) have been identified by NIST SP 800-53B as supporting only availability and may be downgraded to the corresponding control in a lower baseline (or modified or eliminated if defined in a lower baseline) only if the downgrading action reflects the security category for the supported availability security objective defined impact level.

b. Monitor environmental control levels continuously.

2.13.1 PE-14(02) Environmental Controls | Monitoring with Alarms and Notification

Employ environmental control monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment to identified personnel or roles.

2.14 PE-15 Water Damage Protection (L, M, H)

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.

2.14.1 PE-15(01) Water Damage Protection | Automation Support (H)[12]

Detect the presence of water near the system and alert ED designated personnel or roles with Physical Security Program responsibilities using ED approved automated mechanisms such as notification systems, water detection sensors and alarms.

2.15 PE-16 Delivery and Removal (L, M, H)

a. Authorize and control all information system components entering and exiting the facility; and

b. Maintain records of the system components.

2.16 PE-17 Alternate Work Site (M, H)

a. Determine and document the ED approved alternate work sites allowed for use by employees;

b. Employ the following controls at alternate work sites: controls defined within ED directives, policies, including but not limited to ACSD-OCIO-004 *Cybersecurity Policy*, ACSD-OCIO-002[13], *Controlled Unclassified Information Program*;

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.

2.17 PE-18 Location of System Components (H)

Position system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.

[12] PE-15(01) has been identified by NIST SP 800-53B as supporting only availability and may be downgraded to the corresponding control in a lower baseline (or modified or eliminated if defined in a lower baseline) only if the downgrading action reflects the security category for the supported availability security objective defined impact level.

[13] Also known as OCIO: 3-113.

3 RISK ACCEPTANCE/POLICY EXCEPTIONS

Deviations from the Department policies, Instructions, Standards, Procedures or Memos must be approved and documented through the Department's Risk Acceptance process. Deviations that introduce additional risks to the enterprise must be submitted through the Department Risk Acceptance Form (RAF) and must be approved by the ED CISO (as delegated). Requests must justify the reason for the deviation(s)/exception(s) as well as the compensating security controls implemented to secure the device or information, if applicable. Policy deviations that do not introduce additional risks do not need to be submitted through the Department RAF but will need to be approved by the Department CISO (as delegated).

4 ACRONYMS

Acronym	Definition
ACSD	Administrative Communications System Directives
ASHRAE	American Society of Heating, Refrigerating and Air-conditioning Engineers
BOD	Binding Operational Directive
CIO	Chief Information Officer
CISA	Cybersecurity & Infrastructure Security Agency
CISO	Chief Information Security Officer
CSF	Cybersecurity Framework
CT.DP-P	Disassociated Processing
CT-P	Control-P
DE	Detect
DE.CM	Security Continuous Monitoring
DE.DP	Detection Processes
Department	U.S. Department of Education
DHS	U.S. Department of Homeland Security
ED	U.S. Department of Education
EO	Executive Order
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
FTRI	Federal Tax Return Information
GRP	Governance, Risk and Policy
GV.MT-P	Monitoring and Review
GV.PO-P	Governance Policies, Processes, and Procedures
GV-P	Govern-P
H	High
HVA	High Value Asset
IAS	Information Assurance Services
ID	Identify
ID.BE	Business Environment
IRS	Internal Revenue Service
ISO	Information System Owner
ISSO	Information System Security Officer
IT	Information Technology
L	Low
M	Moderate
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
ODP	Organizationally Defined Parameters
OFO	Office of Finance and Operations
OMB	Office of Management and Budget
P	Privacy
PE	Physical and Environmental Protection Family
PF	Privacy Framework
PO	Principal Office

Acronym	Definition
PR	Protect
PR.AC	Identity Management, Authentication and Access Control
PR.AC-P	Identity Management, Authentication, and Access Control
PR.DS	Data Security
PR.DS-P	Data Security
PR.IP	Information Protection Processes and Procedures
PR.PO-P	Data Protection Policies, Processes, and Procedures
PR.PT	Protective Technology
PR.PT-P	Protective Technology
PR-P	Protect-P
PUB	Publication
RAF	Risk Acceptance Form
RS	Respond
RS.AN	Analysis
RS.CO	Communications
SAOP	Senior Agency Official for Privacy
SP	Special Publication

APPENDIX A: BASELINE CONTROL PARAMETER SUMMARY

The applicability for each baseline control parameter is shown below.

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and PF Category	CSF and PF Subcategory
PE-01	Policy and Procedures		X	X	X	PR.AC, PR.IP, DE.DP, GV.PO-P, GV.MT-P, PR.PO-P, PR.AC-P	PR.AC-2, PR.IP-5, DE.DP-2, GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.MT-P2, GV.MT-P6, PR.PO-P4, PR.AC-P2
PE-02	Physical Access Authorizations		X	X	X	PR.AC, PR.AC-P	PR.AC-2, PR.AC-6, PR.AC-P2, PR.AC-P6
PE-02(01)	Physical Access Authorizations | Access by Position or Role					PR.AC, PR.AC-P	PR.AC-2, PR.AC-6, PR.AC-P2, PR.AC-P6
PE-02(02)	Physical Access Authorizations | Two Forms of Identification					PR.AC, PR.AC-P	PR.AC-2, PR.AC-6, PR.AC-P2, PR.AC-P6
PE-02(03)	Physical Access Authorizations | Restrict Unescorted Access					PR.AC, PR.AC-P	PR.AC-2, PR.AC-6, PR.AC-P2, PR.AC-P6
PE-03	Physical Access Control		X	X	X	PR.AC, PR.AC-P	PR.AC-2, PR.AC-P2
PE-03(01)	Physical Access Control | System Access				X	PR.AC, PR.AC-P	PR.AC-2, PR.AC-P2
PE-03(02)	Physical Access Control | Facility and Systems					PR.AC, PR.AC-P	PR.AC-2, PR.AC-P2
PE-03(03)	Physical Access Control | Continuous Guards					PR.AC, PR.AC-P	PR.AC-2, PR.AC-P2
PE-03(04)	Physical Access Control | Lockable Casings					PR.AC, PR.AC-P	PR.AC-2, PR.AC-P2
PE-03(05)	Physical Access Control | Tamper Protection					PR.AC, PR.AC-P	PR.AC-2, PR.AC-P2
PE-03(07)	Physical Access Control | Physical Barriers					PR.AC, PR.AC-P	PR.AC-2, PR.AC-P2
PE-03(08)	Physical Access Control | Access Control Vestibules					PR.AC, PR.AC-P	PR.AC-2, PR.AC-P2
PE-04	Access Control for Transmission			X	X	PR.AC, PR.AC-P	PR.AC-2, PR.AC-P2

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and PF Category	CSF and PF Subcategory
PE-05	Access Control for Output Devices			X	X	PR.AC, PR.AC-P	PR.AC-2, PR.AC-P2
PE-05(02)	Access Control for Output Devices | Link to Individual Identity					PR.AC, PR.AC-P	PR.AC-2, PR.AC-P2
PE-06	Monitoring Physical Access		X	X	X	PR.AC, DE.CM, RS.CO, RS.AN, PR.AC-P	PR.AC-2, DE.CM-2, DE.CM-7, RS.CO-4, RS.AN-1, PR.AC-P2
PE-06(01)	Monitoring Physical Access | Intrusion Alarms and Surveillance Equipment			X	X	PR.AC, DE.CM, RS.CO, RS.AN, PR.AC-P	PR.AC-2, DE.CM-2, DE.CM-7, RS.CO-4, RS.AN-1, PR.AC-P2
PE-06(02)	Monitoring Physical Access | Automated Intrusion Recognition and Responses					PR.AC, DE.CM, RS.CO, RS.AN, PR.AC-P	PR.AC-2, DE.CM-2, DE.CM-7, RS.CO-4, RS.AN-1, PR.AC-P2
PE-06(03)	Monitoring Physical Access | Video Surveillance					PR.AC, DE.CM, RS.CO, RS.AN, PR.AC-P	PR.AC-2, DE.CM-2, DE.CM-7, RS.CO-4, RS.AN-1, PR.AC-P2
PE-06(04)	Monitoring Physical Access | Monitoring Physical Access to Systems				X	PR.AC, DE.CM, RS.CO, RS.AN, PR.AC-P	PR.AC-2, DE.CM-2, DE.CM-7, RS.CO-4, RS.AN-1, PR.AC-P2
PE-08	Visitor Access Records		X	X	X	PR.AC, CT.DP-P, PR.AC-P	PR.AC-2, CT.DP-P2, PR.AC-P2
PE-08(01)	Visitor Access Records | Automated Records Maintenance and Review				X	PR.AC, CT.DP-P, PR.AC-P	PR.AC-2, CT.DP-P2, PR.AC-P2
PE-08(03)	Visitor Access Records | Limit Personally Identifiable Information Elements	X				PR.AC, CT.DP-P, PR.AC-P	PR.AC-2, CT.DP-P2, PR.AC-P2
PE-09	Power Equipment and Cabling			X	X	ID.BE, PR.AC, PR.AC-P	ID.BE-4, PR.AC-2, PR.AC-P2
PE-09(01)	Power Equipment and Cabling | Redundant Cabling					ID.BE, PR.AC, PR.AC-P	ID.BE-4, PR.AC-2, PR.AC-P2

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and PF Category	CSF and PF Subcategory
PE-09(02)	Power Equipment and Cabling | Automatic Voltage Controls					ID.BE, PR.AC, PR.AC-P	ID.BE-4, PR.AC-2, PR.AC-P2
PE-10	Emergency Shutoff			X	X		
PE-11	Emergency Power			X	X	ID.BE, PR.DS, PR.PT, PR.DS-P, PR.PT-P	ID.BE-4, PR.DS-4, PR.PT-5, PR.DS-P4, PR.PT-P4
PE-11(01)	Emergency Power | Alternate Power Supply — Minimal Operational Capability				X	ID.BE, PR.DS, PR.PT, PR.DS-P, PR.PT-P	ID.BE-4, PR.DS-4, PR.PT-5, PR.DS-P4, PR.PT-P4
PE-11(02)	Emergency Power | Alternate Power Supply — Self-contained					ID.BE, PR.DS, PR.PT, PR.DS-P, PR.PT-P	ID.BE-4, PR.DS-4, PR.PT-5, PR.DS-P4, PR.PT-P4
PE-12	Emergency Lighting		X	X	X		
PE-12(01)	Emergency Lighting | Essential Mission and Business Functions						
PE-13	Fire Protection		X	X	X		
PE-13(01)	Fire Protection | Detection Systems – Automatic Activation and Notification			X	X		
PE-13(02)	Fire Protection | Suppression Systems – Automatic Activation and Notification				X		
PE-13(04)	Fire Protection | Inspections						
PE-14	Environmental Controls		X	X	X		
PE-14(01)	Environmental Controls | Automatic Controls						
PE-14(02)	Environmental Controls | Monitoring with Alarms and Notifications						
PE-15	Water Damage Protection		X	X	X		
PE-15(01)	Water Damage Protection | Automation Support				X		
PE-16	Delivery and Removal		X	X	X	PR.DS, PR.DS-P	PR.DS-3, PR.DS-P3
PE-17	Alternate Work Site			X	X		
PE-18	Location of System Components				X		
PE-19	Information Leakage					PR.DS, PR.DS-P	PR.DS-5, PR.DS-P5
PE-19(01)	Information Leakage | National Emissions and					PR.DS, PR.DS-P	PR.DS-5, PR.DS-P5

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and PF Category	CSF and PF Subcategory
	Tempest Policies and Procedures						
PE-20	Asset Monitoring and Tracking					PR.DS, DE.CM, PR.DS-P	PR.DS-3, DE.CM-2, DE.CM-7, PR.DS-P3
PE-21	Electromagnetic Pulse Protection						
PE-22	Component Marking						
PE-23	Facility Location						