BPA Policy 432-1

Physical Security Program

Table of Contents

1. Purpose & Background

To establish the Bonneville Power Administration's (BPA) Physical Security Program in accordance with the Department of Energy (DOE) O 470.4B *Safeguards and Security (S & S),* DOE O 470.3C *Design Basis Threat (DBT),* DOE O 473.3A *Protective Program Operations* and applicable North American Electric Reliability Corporation - Critical Infrastructure Protection (NERC-CIP) standards. This policy will drive a hierarchy of BPA Procedures that incorporate a threat and risk-based approach to protect critical assets, employees, visitors and information against a wide range of threats, including theft, physical attack, sabotage, espionage, unauthorized access, unauthorized release of information, work place violence and other security related events that may negatively affect BPA operations or allow physical harm to employees and visitors.

2. Policy Owner

The Chief Administrative Officer (CAO)**,** working through the Chief Security and Continuity Officer (CSCO) and Supervisory Physical Security Specialist, has the responsibility for ensuring that policies, procedures and safeguards are enacted to protect BPA's mission, employees**,** visitors, S & S interests/assets, and information from harm. For clarification or to have concerns addressed, please contact the Office of Security and Continuity of Operations, at 503-230-3779.

3. Applicability

All employees who meet minimum requirements set forth by DOE and Homeland Security Presidential Directive (HSPD)-12: Policy for a Common Identification Standard for Federal employees and contractors for unescorted access into governmental facilities and have been issued a Personal Identification Verification (PIV) card by BPA or a PIV card issued by another Federal agency; those persons authorized limited access for specific contracted services that are issued a Local Site Specific Only badge; and non-governmental persons who have a validated business need for access and that require an escort**.**

4. Terms & Definitions

A. **Cognizant Security Office (CSO)**: The office assigned responsibility for a given security program or function. At BPA this function resides with the Office of Security and Continuity (OSCO).

B. **Critical Infrastructure**: The term "critical infrastructure" as provided in section 1016(e) of the USA Patriot Act of 2001 (42 U.S.C. 5195c (e)): means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

C. **Energized Facility**: BPA substations, including substation control houses, all buildings included as part of the substation perimeter or contained within the substation and the high-voltage switchyard having energized equipment connected to the high voltage power system.

D. **Essential Elements**: Protection elements necessary for the overall success of the S & S program at a facility or site, the failure of any one of which would result in protection effectiveness being significantly reduced or requires the performance of other elements that exceed the intended utilization in order to mitigate the failure. Essential elements can include but are not limited to equipment, procedures, employees and visitors.

E. **Facility**: A facility consists of one or more S & S interests under a single security management responsibility or authority and a single facility manager within a defined boundary that encompasses all the security assets at that location.

F. **Department of Homeland Security-Interagency Security Committee (DHS-ISC)**: Established through Executive Order 12977 on October 19, 1995, this organization's mandate is to enhance the quality and effectiveness of security for nonmilitary Federal buildings in the United States. The DHS-ISC is responsible for publishing applicable guidelines to federal agencies on a variety of subjects ranging from prohibited items to specific security countermeasures.

G. **North American Electric Reliability Corporation-Critical Infrastructure Protection (NERC- CIP)**: A body of regulatory compliance requirements related to the protection of bulk electric system cyber and physical assets. NERC physical security requirements are primarily captured in the following standards (or their successors): *NERC-CIP 006, Physical Security of Critical Cyber Assets* and *NERC-CIP 014, Physical Security*.

H. **Officially Designated Federal Security Authority (ODFSA)**: A Federal employee designated in writing who possesses appropriate knowledge and responsibilities to carry out actions outlined in the delegation. For BPA, this is the CSCO.

I. **Physical Access Control System (PACS)**: The physical access control system used to allow authorized access and movement of employees, visitors, vehicles, or material through entrances and exits of a secured area. PACS limits access to designated facilities through the use of personally issued electronic access cards that serve as the door and/or gate key.

J. **Safeguards and Security (S & S) Interest/Asset**: A general term for any Departmental/BPA resource that requires protection. The term includes but is not limited to employees/visitors; classified information; Controlled Unclassified Information (CUI) or other Departmental/BPA property.

K. **Site Security Plan (SSP)**: Documents the approved methods for conducting security operations at a facility or site and reflects security operations at that facility or site. The DOE defines a SSP as: "An official document that describes the methodologies,

implementation, and the use of resources by a facility to protect the facility, its sites, and its assets."

L. **Site**: One or more facilities operating under centralized security policies and management, and covered by a site security plan that may consolidate or replace, wholly or partially, individual facility plans.

M. **Video Monitoring Systems (VMS)**: A system that provides the ability to assess security incidents or alarms remotely via cameras.

5. Policy

This policy sets out the requirements for BPA's physical security program. Criteria for BPA's physical security program are derived from DOE orders, the DHS-ISC guidelines and NERC-CIP standards, which when integrated provide the basis for the requirements in this policy.

A. The BPA will establish and maintain a centralized security authority, the Physical Security Office, which supports and facilitates BPA's Mission Essential Function (MEF) of "Deliver electric power in a safe and reliable manner" as stated in BPA's Continuity of Operations Plan. The Physical Security Office is responsible for administering BPA's physical security program. A risk oriented approach is utilized to facilitate the selection of appropriate security measures and optimize limited funding to achieve the required level of security.

1. The Physical Security Office is responsible for enacting and managing a comprehensive physical security program that is risk based and in compliance with these governing DOE orders, DHS-ISC guidelines and NERC-CIP standards:

   a) The DOE's specific standards for protection program operations as described in DOE O 473.3A. This order provides direction on physical security devices (cameras, fencing motions sensors etc.) and security officer qualifications, training and employment.

   b) The DOE's *S & S* program as described in DOE O 470.4B.

   c) The DBT and risk assessment program as described in DOE O 470.3C.

   d) NERC-CIP standards that are related to the Federal Columbia River Power System (FCRPS); specifically energized facilities and associated control centers.

   e) Security standards concerning GSA leased and owned buildings are found in DHS-ISC guidance documents, such as *Items Prohibited from Federal Facilities* and *Physical Security Criteria for Federal Facilities.*

2. The Physical Security Office will employ a risk based approach that incorporates the systematic collection and analysis of threat information, and will:

   a) Ensure an effective threat management program able to identify and monitor potential threats.

b) Act in collaboration with DOE Counterintelligence, local and national law enforcement, state intelligence fusion centers and other Federal agencies as detailed in BPA Procedure 432-1-7 *Threat Management Program.*

3. The Physical Security Office will develop and maintain a security risk assessment program that fulfils DOE orders, NERC-CIP standards and DHS-ISC guidelines, and will:

   a) Ensure the selection of security risk assessment methodology or methodologies.

   b) Ensure that security risk assessment requirements and applicability are documented in BPA Procedures 432-1-2 *Critical Asset Security Plan* and 431-1-8 *Design Basis Threat.*

4. The ODFSA and CSO provide guidance and direction for the following responsibilities.

   a) Standardized and effective physical access control systems are used at areas identified as controlled access.

   b) All facilities with controlled access are consistent with issuance, revocation, and assessment of physical access privileges for all employees and visitors**.**

   c) Documentation of procedures, enforcement of rules, and assessment of effectiveness of procedures.

   d) Enforcement of the prohibition on controlled items, firearms and other prohibited items inside GSA-leased and BPA facilities in accordance with 18 U.S.C. § 930: Possession of firearms and Dangerous weapons in Federal facilities and as expounded upon in BPA Procedure 432-1-3 *Controlled Items, Firearms and other Prohibited Items*.

   e) Development and maintenance of budgetary support for the incorporation of the Essential Elements into an *S & S* program that is tailored to BPA's MEF of "Deliver electric power in a safe and reliable manner."

B. BPA's strategic direction drives priorities for its physical security program.

   1. Security projects that enhance the operability of the FCRPS must undergo a business case review that clearly demonstrates the proposed security system's cost effectiveness to achieve the greatest reduction in risk.

   2. Enacted security practices and countermeasures must demonstrate alignment with BPA's strategic direction.

   3. Protection strategies for BPA's critical assets as required in DOE orders, DHS-ISC and NERC-CIP standards are outlined in BPA Procedure 432-1-2 *Critical Asset Security Plan* and BPA's Security Asset Management Strategy.

C. The Physical Security Office as BPA's lead for physical security ensures the following:

1. Effective physical protection strategies are developed, promulgated and enforced that protect critical infrastructure, and *S & S* interests/assets from unauthorized access, unauthorized use, sabotage, theft and/or vandalism.
2. Performance requirements are documented for the security services contract and security officer's assigned protective duties, in accordance with *DOE*, federal and state requirements.
3. Safeguards and security programmatic responsibilities and BPA procedures promulgated from the CSO and ODFSA are documented and approved.

6. Policy Exceptions

There are no exceptions related to this policy.

7. Responsibilities

A. Administrator and Chief Executive Officer: Responsible for the overall security and safety of BPA employees and visitors and the protection of BPA's S & S interests/assets in accordance with DOE orders, DHS-ISC guidelines, and NERC-CIP standards. The Administrator shall delegate in writing ODFSA and security authority to the CSCO for all S & S responsibilities.

B. Chief Administrative Officer: Exercises administrative control over all aspects of the BPA Physical Security program. Responsible for ensuring compliance with applicable DOE orders, DHS-ISC guidelines and NERC-CIP standards. Acts as the sponsor for the BPA Local Insider Threat Working Group (LITWG).

C. Chief Security and Continuity Officer: Through delegation, performs as the ODFSA for BPA. Ensures S & S related directives, procedures, programs and standard operating practices are developed, coordinated, and promulgated throughout the agency. Responsible for implementation of all S & S requirements as identified by DOE, NERC-CIP, and DHS-ISC as it applies to protection of people, information, and facilities. Responsible for ensuring this Physical Security Policy and program contain the following Essential Elements:

1. Procedures to manage violations of internal security policy or procedures. *BPA Procedure 432-1-2, Appendix D – Failure to Follow Security Policies or Procedures* outlines procedures for suspension of access privileges to BPA S & S interests/assets after three or more security violations in a 12 month period, or immediate suspension for a severe incident, as well as remediation procedures. The ODFSA has authority to suspend physical access privileges pending further investigation for employees and visitors who may pose a risk to the Agency.
2. Development of SSPs in accordance with DOE orders for identified facilities.

3. Documented visitor control program in accordance with DOE orders, DHS-ISC and NERC-CIP standards, to include requirements for escorting at non-energized and energized facilities.
4. Physical security planning, scoping, design-support, and implementation in accordance with capital or expense project processes as appropriate. Track compliance with the *Security Asset Management Strategy* implementation plan.
5. Acts as the senior manager responsible for authorizing and directing contract security officer resources during emergency situations.
6. Documented random employee inspection program, in partnership with Federal Protective Service.
7. Documented implementation plan of DOE's DBT program.
8. Acts as the Chair of the LITWG.

D. Supervisory Physical Security Specialist: Responsible for overall management and implementation of the BPA Physical Security Program and associated budget. Ensures compliance and enforcement of all applicable DOE orders, DHS-ISC and NERC-CIP standards and local, state, and Federal statutes. Provides direct managerial oversight and execution of the following goals and objectives:

1. Establish and document physical security standards associated with critical infrastructure (See E. below).
2. Liaison with the Federal Protective Service, other Federal agencies and Local and State law enforcement entities.
3. Development and review of SSPs for identified facilities.
4. Development and review of procedures to prevent the introduction of firearms, explosives and prohibited items unto and into BPA's facilities and sites as required by 18 U.S. Code and DOE Orders.
6. Development, implementation and enforcement of the BPA Visitor Control program.
7. Documented key control program procedures for internal BPA organizations.
8. Oversee the security awareness and reporting program as part of a comprehensive threat management program.
9. Compliance with and enforcement of all physical security-related NERC-CIP standards for critical infrastructure, assets and supporting programs.
10. Coordinate with BPA Aircraft Services in formulating agency level guidance concerning aviation that directly affects physical security.
11. Enforcement of all applicable DHS-ISC requirements as related to the physical security of BPA's non-energized facilities.

12. Documented procedures for recording, responding and reporting security incidents.
13. Coordinated procedures between BPA Human Capital Management, Employee Relations and Physical Security regarding crisis intervention and employee misconduct investigations.
14. Provides oversight of maintenance budget for Physical Access Control and Monitoring Team (JS) execution associated with PACS and VMS and sets priorities for the maintenance of the aforementioned systems.
15. Sets overall physical protective system requirements for transmittal to JS for implementation.
16. Key member of the BPA's LITWG.
17. Responsible for oversight of physical security risk assessments and risk management for NERC-CIP facilities and sites, BPA owned and operated and GSA leased buildings.
18. Document competency and proficiency standards for Physical Security Specialists to ensure staff are trained and equipped to execute this policy.

E. Physical Security Specialist, Program Manager: Responsible for researching, documenting and codifying physical security standards.

1. Establishes agency level physical security requirements and standards for fencing, lighting, gates, intrusion detection and other physical security measures.
2. The Physical Security Office's main point of contact for collaboration and coordination with Transmission Services for new construction, major renovations and security enhancement projects associated with critical infrastructure and assets owned by Transmission Services.

E. All Managers shall:

1. Be knowledgeable of physical security rules and procedures and their application at BPA.
2. Ensure direct reports comply with all site specific security requirements, procedures and policies.
3. Promptly address concerns or identified security violations related to this policy with employees and provide corrective actions in a timely manner.
4. Ensure direct reports complete required security related training.
5. Advise the OSCO of any changes to operations or facilities which may impact security and/or require an alteration of security plans, systems, procedures or practices.
6. Promptly report changes in employee access requirements.

7. Promptly communicate to Physical Security all employee matters related to violence, violation of security procedure, theft, concerns of harm to others/self or other adverse information (arrests, convictions, etc.).
8. Ensure that employees adhere to BPA Procedure 432-1 *Critical Asset Security Plan*, *Appendix D – Failure to Follow Security Polices or Procedures.*

F. All employees shall:

1. Promptly report all security incidents (suspicious or actual) and threats.
2. Never tamper with, alter, impede, bypass or otherwise circumvent security devices, systems, procedures or policies.
3. Comply with all site specific security requirements, procedures, and policies in accordance with applicable DOE orders and NERC CIP standards.
4. Properly protect S & S interests/assets. This includes those items in the employee's direct control as well as issued identification badges and keys that provide access.
5. Perform all actions associated with visitor and escort responsibilities for hosted guests requiring building access.

G. Physical Access Control and Monitoring Team (JS) shall, as the system owner for PACS and VMS:

1. Implement physical protection system requirements as set by Supervisory Physical Security Specialist.
2. Provide technical expertise and oversight for installation and maintenance of PACS and VMS.
3. Coordinate budget and work priorities with the Supervisory Physical Security Specialist.

H. Transmission Services – Transmission Business Line Shall

1. Advise the CSCO of changes to Project Requirements Diagram, engineering standards, substation, facilities or civil designs which may impair security and/or require an alteration of security plans or security systems, procedures or practices.
2. Communicate to the CSCO procedures and process related to NERC-CIP that may impact safeguards and security operations.
3. Comply with all applicable DOE orders and NERC-CIP security standards.

8. Standards & Procedures

For more detailed guidance on the specific procedures, roles and responsibilities for each program area please refer to the following:

A. BPA Procedure 432-1-1 *Protective Forces*

Establishes requirements for the management and operation of BPA contracted protective forces. Which describes the integration of physical security measures and protective forces other S & S programs such as program planning, and management and information security.

B. BPA Procedure 432-1-2 *Critical Asset Security Plan* (CASP)

The CASP provides detailed guidance and procedures related to BPA's strategy for the implementation of Department of Energy (DOE) *Order 470.4B, Safeguards and Security Program* to protect and monitor critical assets. This procedure supports the implementation of *DOE Order 470.3C, Design Basis Threat,* the NERC-CIP Standards, and HSPD-12.

C. BPA Procedure 432-1-3 *Controlled Items, Firearms, and Other Prohibited Items*

This procedure establishes guidelines governing the possession, transportation, storage, or use of firearms, other deadly weapons, explosive devices and other items prohibited on BPA property, in Government vehicles or in private vehicles located on BPA property or used in the conduct of BPA business.

D. BPA Procedure 432-1-4 *Criminal and Threat Reporting*

Establish policy and procedures for individuals possessing an access authorization to report possible attempts by hostile intelligence services to obtain sensitive BPA information or technology. Additionally, this policy establishes overall policy for all Bonneville employees, regardless of possession of an access authorization or not, with responsibility for reporting hostile contacts attempting to access agency critical and sensitive information without authorization.

E. BPA Procedure 432-1-5 *Visitors*

Describes site specific requirements and processes for receiving visitors. Primarily for person(s) who does not possess a HSPD-12 Personal Identification Verification credential along with guidance on escorting procedures including notification, logging and badging requirements. This procedure offers guidance concerning Military and other Federal and agency employees in possession of HSPD-12 badges provided by their parent organizations.

F. BPA Procedure 432-1-6 *Key Control*

Establishes a program to protect and manage locks and keys. Security locks and keys are devices used to secure movable barriers and can include electrical or mechanical locks and keys, key cards, access codes, and other non-standard locking devices. A lock and key program is applied to S & S interests being protected, existing barriers, and other protection measures afforded these interests.

G. BPA Procedure 432-1-7 *Threat Management Program*

Establishes the BPA Threat Management Program in accordance with DOE O 470.4B Safeguards and Security Program and NERC-CIP-014, Requirement 3, the evaluation of potential threats and vulnerabilities of a physical attack. This policy provides managers and staff situational understanding of the threats facing BPA employees and visitors and assets. Threat management is a continuous process that facilitates situational understanding for decision makers. It supports the planning, preparation, and execution of operations by allowing managers to focus resources on the most likely threats and lessen the complexity of trying to develop a strategy to defend against all threats. This reduces cost, allowing resources to be redirected to redundancy and resiliency projects. Threat Management also supports the Security and Safeguard function by alerting managers to potential and emerging threats which will assist in preserving and protecting employees, visitors, and equipment.

H. BPA Procedure 432-1-8 *Design Basis Threat*

Establishes the BPA approach to the implementation and programmatic management of requirements found in DOE-O-470-3C. This procedure defines the agency approach to conducting required Security Risk Assessments (SRA) and the application of security risk management principles and corresponding protection strategies; establishing the BPA's approach to categorizing assets and prioritizing resources. Defines and explains a framework for long-term security system design based on the consistent application of SRA methodologies, commonly defined threats and reasonably expected outcomes. Finally, provides guidance for the implementation of applicable security measures, based on security risk management, which forms the basis for security system planning in an environment of limited funding and resources.

9. Performance & Monitoring

Policy and program effectiveness are assessed through the annual NERC-CIP certification process, DOE self-assessment reporting for S & S topical areas, and OSCO annual internal self-assessment activities for S & S programs. Through these established efforts, OSCO is able to monitor S & S effectiveness, efficiency, and compliance to DOE and NERC-CIP security related requirements. Additionally, OSCO is able to assess the performance of the layers of security and related programmatic areas.

A. Limited scope performance testing and alarm response assessment performance testing will be utilized to assess the contracted security provider for adherence to security procedures, contractual requirements and the statement of work.

B. JS will utilize reporting mechanisms in collaboration with OSCO for prioritizing work, scheduling work and the resolution of reported PACS and VMS deficiencies.

C. Regional Security Specialists are responsible for the status of physical security program and essential elements inside their regions.

D. All Physical Security Specialists in general are responsible for the implementation, enforcement and monitoring of all applicable DOE orders, NERC-CIP standards and Local, State, and Federal laws and regulations.

10. Authorities & References

A. DOE 470.4B *Safeguards and Security*

B. DOE O 470.3C *Design Basis Threat (DBT)*

C. DOE O 473.3A *Protective Program Operations*

D. North American Electric Reliability Corporation-Critical Infrastructure Protection standards

E. HSPD – 7: U.S. national policy for identification of and prioritization for protection of critical infrastructure

F. HSPD – 12: Policy for a Common Identification Standard for Federal Employees and Contractors

G. 18 U.S.C & 930: Possession of firearms and Dangerous weapons in Federal facilities

11. Review

A. This policy will be reviewed and updated within 90 days of the effective date of a new version of DOE policy and orders affecting the S & S Program.

B. This policy will be reviewed and updated within 90 days of an internal reorganization that affects any entity in the roles and responsibilities section.

C. This policy will be reviewed every 5 years by the CSO.

12. Revision History

Version Number	Issue Date	Brief Description of Change or Review
1.0	8/2/2019	New Policy