BPA Policy 430-1

Safeguards and Security Program

Security and Continuity of Operations

Table of Contents

430-1.1 Purpose and Background

To establish BPA's Safeguards and Security (S&S) Program planning and management requirements in accordance with DOE O 470.4B Safeguards and Security Program and DOE 470.3B Graded Security Plan (GSP). S&S policies and programs will incorporate risk-based approach to protect assets and activities against consequences of attempted theft, diversion, attack, sabotage, espionage, unauthorized access, compromise and other acts that may have an adverse impact on operations. S&S policies and programs apply to all BPA facilities and sites (owned or leased).

430-1.2 Policy Owner

The Administrator and Chief Executive Officer, working through the Chief, Security and Continuity Officer, has overall responsibility for ensuring adequate safeguards and security policies and programs to prevent unacceptable adverse impacts on national security, the health and safety of BPA and contractor workers, the public, or the environment. For questions or inquiries, please contact the Office of Security and Continuity of Operations, at 503-230-3779.

430-1.3 Applicability

All BPA personnel with authorized and unescorted physical access to BPA facilities and information systems.

430-1.4 Terms and Definitions **(see BPA Dictionary for terms and definitions not included in this section: http://powerweb.bpa.gov/definitions/index.asp)**

A. **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. These requirements are currently captured in NERC CIP 006: Physical Security of Critical Cyber Assets and NERC CIP 014: Physical Security.

B. **Cognizant Security Office (CSO):** Cognizant security office means the office assigned responsibility for a given security program or function. Where DOE cognizant security office is stated, the reference is to a Federal activity.

C. **Control System Monitoring (CSM)/Network and System Operations Center (N-SOC):** The Network and System Operations Center (N-SOC) Program supports 24/7 Control Center operations and monitoring functionality. It is based on an industry common best practice operations model of a service and command center and an automation center, which controls the management tools used within the operations center. The service and command center is divided into two functions that will complement each other and work in tandem, the NOC and SOC. Its mission is to provide continuous Network and System monitoring, incident response, IT support, remedial action, and incident coordination.

D. **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.

E. **Critical Infrastructure Protection (CIP):** The protection of identified critical infrastructure, including cyber and physical assets, in support of reliability of the BPA Transmission System and operations and NERC CIP.

F. **Department of Homeland Security (DHS):** DHS has oversight over the security management of government buildings and issues mandates for physical access controls for all Federal buildings that BPA must comply with such as Homeland Security Presidential Directive (HSPD) 7 and HSPD 12.

G. **Energy Facility:** In accordance with Title 18 USC, means a facility that is involved in the production, storage, transmission, or distribution of electricity, regardless of whether such facility is still under construction or is otherwise not functioning. BPA defines the energy delivery facility as existing or planned location or site, encompassing all real property and appurtenances, at which a BPA substation, switching station, transmission line or radio station is located.

H. **Essential Elements:** Protection and assurance 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 which would require performance of other elements to be significantly better than expected in order to mitigate the failure. Essential elements can include but are not limited to equipment, procedures, and personnel.

I. **Facility:** A facility consists of one or more S&S interests under a single security management responsibility or authority and a single facility security officer within a defined boundary that encompasses all the security assets at that location. A facility operates under a security plan that allows security management to maintain daily supervision of its operations, including day-to-day observations of the security program.

J. **Facility Security Officer (FSO):** A DOE, badged worker that is a U.S. Citizen with a security clearance equivalent to the facility clearance or higher, who is assigned the responsibility of administering the requirements of the safeguards and security program at the facility.

K. **Site Security Plan (SSP):** The SSP documents the approved methods for conducting security operations at a facility or site and therefore must reflect security operations at that facility or site at all times. The plan must describe in detail, either in its content or in combination with other explicitly referenced documents, all aspects of

S&S operations occurring at the location and must include documentation of any deviations from national or DOE requirements. From DOE, the definition is: 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. **Insider:** Any person with authorized access to any government or contractor resource to include personnel, facilities, information, equipment, networks, or systems.

M. **Insider Threat:** The threat that an insider will use his/her authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the US through espionage, terrorism, unauthorized disclosure of classified information, or through the loss or degradation of US Government resources or capabilities.

N. **North American Electric Reliability Corporation** (**NERC):** North American Electric Reliability Corporation is a not-for-profit international regulatory authority whose mission is to ensure the reliability of the bulk power system in North America. NERC develops and enforces Reliability Standards; annually assesses seasonal and long-term reliability; monitors the bulk power system through system awareness; and educates, trains, and certifies industry personnel.

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

P. **Safeguards and Security (S&S) Interest/Asset:** A general term for any Departmental/BPA resource or property that requires protection from malevolent acts. It includes but is not limited to personnel; classified information; sensitive unclassified information or other Departmental/BPA property.

Q. **Security Condition (SECON) Levels:** SECON levels are used by DOE to establish the current security readiness state (DOE O 470.4B), and reflect a multitude of conditions that may adversely impact Departmental and/or facility and site security. SECONs range from Level 1 (most severe) through 5 (lowest) and include terrorist activity, continuity conditions, environmental (fire, chemical, radiological, etc.) and/or severe weather conditions. The day-to-day DOE security readiness state is informed by the Homeland Security National Terrorism Advisory System (NTAS). NTAS alerts are established based on the analysis of a continuous and timely flow of integrated, all-source threat assessments and reporting provided to Executive Branch decision-makers.

R. **Security L/Q Clearance:** An administrative determination that an individual is eligible for access to classified matter and/or special nuclear material. In DOE and NRC, security clearances are designated as Q and L. Security clearances at other

Federal agencies are designated as Top Secret, Secret, or Confidential indicating that the recipient is approved for access to National Security Information or Formerly Restricted Data at a classification level equal to or less than his/her security clearance level.

S. **Site:** A site consists of one or more facilities operating under centralized security management, including a site security officer (Facility Security Officer) with consolidated authority and responsibility for the facilities, and covered by a site security plan that may consolidate or replace, wholly or partially, individual facility plans.

T. **Video Monitoring Systems (VMS):** The video monitoring system provides security's Alarm Monitoring Station (AMS) the ability to assess security incidents or alarms remotely via cameras.

430-1.5 Policy

A. BPAs Safeguards and Security Program Planning and Management policies are derived from the following DOE orders and the North American Electric Reliability Corporation (NERC):

1. Safeguards and Security (S&S) Program as described in DOE Order 470.4B
2. Graded Security Protection (GSP) Policy, DOE Order 470.3B
3. Insider Threat Program, DOE Order 470.5
4. North American Electric Reliability Corporation Critical Infastructure Protection (NERC-CIP)

B. These policies provide overall requirements for the following:

1. Protect Government property and interests from unauthorized access, use, sabotage, theft or vandalism.
2. Protect classified information and assets.
3. Comply with all Department of Energy Directives, Department of Homeland Security Directives, North American Electric Reliability Corporation and other security regulations as may be required.
4. All safeguards and security programmatic responsibilities and procedures shall be approved and promulgated from the cognizant security office responsible for implementing BPA's security program.
5. Ensure that S&S personnel are managed, trained, and equipped and are provided resources and support services needed to maintain protection of S&S interests.

430-1.6 Policy Exceptions

There are no exceptions related to this policy. The policies for Information Security, Foreign National Visits and Assignments, Personnel Security and Identity Credential and Access Management are covered under separate policy.

430-1.7 Responsibilities

430-1.7.1 Chief, Security and Continuity Office (CSCO) shall:

A. As a DOE Cognizant Security Office and Facility Security Officer, coordinates and promulgates the Agency's policies and procedures for a comprehensive Safeguards and Security (S&S) Program as described in DOE Order 470.4B Safeguards and Security Program; DOE Order 470.3B Graded Security Protection Policy; and DOE Order 470.5 Insider Threat Program . The BPA S&S Program shall contain the following elements:

1. S&S Program Planning
2. Development and ongoing review and update of Site Security Plans
3. Development and ongoing review of Security Conditions (SECON) levels, planning and coordination
4. BPA Security Performance Assurance Program
5. BPA S&S Survey and Self-Assessment Program
6. BPA S&S Facility Clearance Registration
7. BPA S&S Training and Awareness Program
8. BPA's Incidents of Security Concern Program and Security Incident Response Plan
9. BPA's Insider Threat Program

B. Develops BPA's S&S Program in consonance with DOE and the Department of Homeland Security (DHS) requirements as well as North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards.

C. Perform duties as the Federal approving official in accordance with DOE O 470.4B Safeguards and Security Program, Facility Clearances and Registration of Safeguards and Security Activities, Section 1.2, for all facility and site security plans.

D. Implements the requirements for use of guard force protection for sites and facilities as needed. Senior Manager responsible for authorizing and directing guard force resources during emergencies situations.

E. Is the senior manager for implementation of NERC CIP standards associated with physical security, information protection and personnel risk assessments. These duties include, but are not limited to, upgrades at existing facilities, including funding, project planning, scoping, design-support, implementation and final acceptance.

F. Perform S&S planning, scoping, design-support, and implementation in accordance with capital or expense project processes as appropriate. Track compliance with security asset management strategy implementation plan.

430-1.7.2 All Employees shall:

A. Complete Annual Security Refresher training.

B. Report all security incidents (suspicious and actual) and threats in accordance with prescribed procedures.

C. Never tamper with, alter, impede, bypass or otherwise circumvent security devices, systems, procedures or policies.

D. Comply with all site specific security requirements, procedures, and policies. (Example:NERC CIP)

430-1.7.3 Managers shall:

A. Ensure a unified line-management approach by maintaining knowledge and practice of S&S rules and procedures.

B. Promptly address S&S concerns with employees and provide corrective actions in a timely manner.

C. Ensure direct reports complete required training.

D. Ensure direct reports comply with all site specific security requirements, procedures and policies (Example: NERC CIP).

E. Shall advise Chief, Security and Continuity Office of changes to operations or facilities which may impair security and/or require an alteration of Security Plans systems, procedures or practices.

430-1.7.4 Human Capital Management shall:

A. Ensure all covered positions within BPA are at a high, moderate, or low risk level as determined by the position's potential for adverse impact, to ensure appropriate investigations are completed and appropriate security controls and monitoring are applied.

B. Complete suitability adjudication in accordance with Office of Personnel Mangement standards to ensure all issues of a concern are properly addressed and mitigated. Also applies suitability reviews for positions requiring reinvestigations.

C. Maintain accurate and complete employee training records that contain dates of course attendance, course title, and scores/grades achieved (where applicable) in accordance with DOE Administrative Records Schedule 1, Personnel Records.

D. Establish standards for development and delivery of security training and collaborate with training owners to ensure timely delivery and relevant training material is used.

E. Support the Local Insider Threat Work Group initiatives.

430-1.7.5 Information Technology shall:

A. Be responsible for Software Development and Operations.

B. Perform duties of Information System Owner (ISO) and Information System Security Officer (ISSO), responsible for maintenance of the Physical Access Control System (PACS) and Video Monitoring Systems (VMS).

C. Responsible for ensuring PACS and VMS meets compliance requirements in accordance with Federal Information Security Management Act (FISMA), North American Electric Reliability Corporation (NERC) and Homeland Security Presidential Directives (HSPD).

D. Responsible for installation and maintenance of PACS and VMS. Coordinates engineering, design, approval and installation and maintenance with appropriate Transmission Service organizations.

430-1.7.6 Transmission Services - Transmission Business Line shall:

A. Advise Chief, Security and Continuity Office 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 systems, procedures or practices.

B. Communicate to CSCO procedures and processes related to NERC CIP that may impact safeguards and security operations.

430-1.8 Standards & Procedures

430-1.8.1 Safeguards and Security Program Planning:

Will incorporate a planning approach that will provide facilities and sites with consistent method for identifying, developing and documenting sound risk mitigation strategies by identifying all critical S&S performance, technical, schedule and cost elements. S&S planning activities are conducted to ensure that identified S&S assumptions and operating conditions used to formulate plans are adequate to protect BPA S&S interests and assets, as well as the public, employees, from malevolent actions. S&S related planning and associated activities are the responsibility of the Facility Security Officer/Cognizant Security Office.

A. Planning activities shall be in alignment with the DOE Strategic Plan, BPA's mission and strategic business objectives, as well as projected operational and fiscal constraints.

B. Ensure ongoing review and approval of BPA's Site Security Plans and that they accurately describe site/facility S&S procedures and requirements.

C. Ensure assessments of protection effectiveness are conducted at a level of rigor appropriate to the asset/interest being protected.

D. Develop and document BPA Security Condition (SECON) response plans that can be immediately implemented.

E. Develop Incidents of Security Concern plan in accordance with DOE guidance.

F. Develop BPA's Insider Threat Program and co-lead BPA's Insider Threat Working Group, supporting DOE's goal to deter, detect, and mitigate insider threat actions by Federal and contractor employees. Program will apply to all programs in an integrated manner to address threats to personnel, facilities, information, equipment or other government assets.

430-1.8.2 Site Security Plans:

A. All facilities and sites under DOE cognizance must have a Site Security Plan (SSP) that reflects the assets, security interests, and approved S&S program implementation at that location and any residual risks associated with operation under the security plan.

1. For those facilities that do not have security assets (e.g., classified information or matter, or other assets requiring a facility security clearance (FCL)), the SSP must be developed to address the protection of employees and Government-owned and/or leased property.

2. The following security planning activities shall be accomplished for all applicable facilities and sites:

(i) SSPs shall provide assurances for safeguarding against loss, theft, diversion, unauthorized access, misuse, or sabotage that could adversely affect national security and the health and safety of employees, the public, and the environment in accordance with DOE O 470.3B, *Graded Security Protection (GSP) Policy*, and DOE O 231.1B, AdminChg 1, *Environment, Safety and Health Reporting*.

(ii) Security planning activities are completed in a timely manner to ensure that security risks are mitigated at all times in accordance with agency safeguards and security standards.

(iii) Security planning supports the facility's/site's mission, forecasts of significant changes to facility/site operations, and current and projected operational and fiscal constraints.

(iv) Site operations are conducted in compliance with approved SSPs.

(v) Progress on completion of implementation plans is monitored by an approved Federal official to ensure that approved actions are completed within the approved time frames.

(vi) Assessments of protection effectiveness are conducted at a level of detail and rigor appropriate to the assets and security interests being protected and in accordance with national standards and DOE directives, and ensure that documentation of such analyses are maintained in support of the security plan.

B. BPA shall publish SSPs for the following sites and facilities:

1. Ross Complex, including Dittmer Control Center
2. Munro Complex, including Munro Control Center
3. Headquarters
4. Aircraft Services
5. Celilo
6. Vancouver Mall
7. Regional Security Plans describing duties and responsibilities of the regional offices, districts and the CSCO.
8. Critical Asset Security Plan to describe agency risk assessment strategies and the implementation plan for upgrading Transmission Critical Assets.
9. Other facilities as deemed appropriate by the CSCO.

430-1.8.3 Security Condition (SECON) levels, planning and coordination:

The Department of Energy establishes the overall policies for Security Condition levels. BPA OSCO implements SECON levels in accordance with DOE policy. SECON levels reflect a multitude of conditions that may adversely impact a facility, its operations or site security. SECONs may include terrorist activity, continuity conditions, environmental and/or severe weather conditions. Specific procedures and instructions for BPA's SECON levels are described in Procedures 430-1-4.

The Office of Security and Continuity of Operations, Chief Security and Continuity Officer is responsible for developing, updating, and communicating information related to Security Conditions including documenting BPA's Security Conditions procedures. The Chief, Office of Security and Continuity of Operations may elevate Security Conditions

based on national situation reports, security intelligence, or BPA specific events or threats.

Site managers (e.g. Regional or District Managers, Chief Substation Operators) may increase site Security Conditions from time to time to address immediate and unexpected events or emergencies.

430-1.8.4 Performance Assurance Program

The Department of Energy establishes the overall policies for acceptable levels of performance that shall be maintained to ensure that all elements of a site protection program are workable and function as designed and in accordance with overall protection goals established by FSO. Performance Assurance Program shall identify the essential elements of the protection program and establishes monitoring and testing activities with sufficient rigor to ensure program elements are at all times operational, functioning as intended, and interacting in such a way as to identify and preclude the occurrence of adverse activity before security is compromised. BPA's specific procedures are described in System Performance and Assurance Testing Program found in Procedures 430-2, System Performance and Assurance Testing Program.

430-1.8.5 Survey, Review and Self-Assessment Program

The Department of Energy establishes the overall policies for surveys, reviews and self-assessments programs and requirements. BPA's programs shall provide assurances to DOE that safeguards and security interests and activities are protected at the required levels. Additionally, such programs shall provide the FSO and cognizant security office with the information necessary to make informed decisions regarding the allocation of resources, acceptance of risk, and mitigation of S&S vulnerabilities. OSCO conducts assessments in accordance with DOE guidance and models activities described under the Periodic Survey Program. BPA's specific procedures for surveys, reviews and self-assessments are described in Procedures 430-3.

430-1.8.6 Facility Clearance Registration (Appendix B, Section 1 of DOE 470.4)

BPA shall follow DOE policy for Facility Clearance Registrations to ensure that DOE, DOE contractor, and other (Federal) government agency (OGA) facilities and their contractors engaged in DOE activities are eligible for access to, and meet the requirements to possess and secure, classified information; and, as applicable, to protect other assets and conduct other security activities on behalf of DOE.

430-1.8.7 Safeguards and Security Awareness and Training

A. The BPA Safeguards and Security awareness program:

1. Is responsible for communicating personal security responsibilities to all individuals at a facility or site (anyone with unescorted access). Additional training and

awareness actions are required for persons with access to classified information (possess a security L/Q clearance).
2. An initial security briefing for all individuals who are issued a DOE security badge.
3. Comprehensive, refresher, and termination briefings for all individuals with a DOE security clearance (L/Q) for access to classified information.
4. Appropriate site-specific awareness information for other BPA personnel granted unescorted access to facilities and work areas.

B. Annual S&S refresher briefings must address BPA site-specific knowledge and needs, BPA S&S interests, and potential threats to the facility/organization.

C. Contents must be reviewed regularly and updated as necessary.

430-1.8.8 Incidents of Security Concern

Department of Energy establishes policies associated with reporting of security incidents throughout the Department. BPA's OSCO shall ensure appropriate development of security incident prompts, to include an assessment of the potential impacts, appropriate notification, extent of condition, and corrective actions. BPA's specific procedures associated with this policy are found in Procedures 430-5.

430-1.8.9 Insider Threat Program

The BPA Local Insider Threat Program will operate in accordance with DOE described objectives as outlined in DOE Order 470.5 and published guidance. Specific BPA procedures are described in Procedures 430-6. The BPA Local Insider Threat Program:

1. Will coordinate with Denver Senior Counter intelligence Officers, who performs as co-sponsor of BPA's Local Insider Threat Working Group (LITWG) .
2. Will appropriate develop and integrate insider threat related policies and procedures across BPA as needed (e.g. Human Capital Management, Supplemental Labor).
3. Will develop appropriate information sharing tools to properly identify, collect and process data required to address insider threats.
4. Will ensure appropriate development of Insider Threat Working Group, comprised of representatives from HCM, Transmission Services, Substation Operations, Security, and Cyber Security.
5. Establish, maintain and conduct training and awareness activities to ensure employees are informed of their responsibilities.
6. Assist in preparing annual progress/status report to DOE.

430-1.9 Performance and Monitoring

Policy and program effectiveness will be assessed through the annual NERC CIP certification process, DOE self assessment quarterly reporting for safeguards and security topical areas, and OSCO's 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 programs areas.

430-1.10 Authorities and References

1. DOE O 470.4B Safeguards and Security Program
2. DOE O 470.3B Graded Security Protection (GSP) Plan
3. DOE O 470.5 Insider Threat Program
4. DOE O 470.2 Safeguards and Security Independent Oversight Program

430-1.11 Review

1. 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.
2. This policy will be reviewed and updated within 90 days of an internal reorganization that affects any entity in the roles and responsibilities section.
3. This policy will be reviewed every 5 years by the cognizant security authority.

430-1.12 Revision History

Draft Date	Description
July 2015	Original Policy Finalized