CONTRACTOR COMPLIANCE WITH BONNEVILLE POLICIES (MAR 2018)

(a) The contractor shall comply with all Bonneville policies affecting the Bonneville workplace environment. Examples of specific policies are:
(1) Bonneville Smoking Policy (Bonneville Policy 440-1),
(2) Use of Alcoholic Beverages, Narcotics, or Illegal Drug Substances on Bonneville Property or When in Duty Station (BPAM 400/792C),
(3) Firearms and Other Weapons (BPAM 1086),
(4) Standards of conduct regarding transmission information (BPI 3.2),
(5) Identification Badge Program (Bonneville Security Standards Manual, Chapter 200-3)
(6) Information Protection (Bonneville Policy 433-1),
(7) Safeguards and Security Program (Bonneville Policy 430-1);
(8) Managing Access and Access Revocation for NERC CIP Compliance (Bonneville Policy 430-2);
(9) Cyber Security Program (Bonneville Policy 434-1),
(10) Business Use of Bonneville Technology Services (BPAM Chapter 1110),
(11) Prohibition on soliciting or receiving donations for a political campaign while on federal property (18 U.S.C. § 607),
(12) Guidance on Violence and Threatening Behavior in the Workplace (DOE G 444-1-1),
(13) Inspection of persons, personal property and vehicles (41 CFR § 102-74.370),
(14) Preservation of property (41 CFR § 102-74.380),
(15) Compliance with Signs and Directions (41 CFR § 102-74.385),
(16) Disturbances (41 CFR § 102-74.390),
(17) Gambling Prohibited (41 CFR § 102-74.395),
(18) Soliciting, Vending and Debt Collection Prohibited (41 CFR § 102-74.410),
(19) Posting and Distributing Materials (41 CFR § 102-74.415)
(20) Photographs for News, Advertising or Commercial Purposes (41 CFR § 102-74.420), and
(21) Dogs and Other Animals Prohibited (41 CFR § 102-74.425).

(b) The contractor shall obtain from the CO information describing the policy requirements. A contractor who fails to enforce workplace policies is subject to suspension or default termination of the contract.

BPA Policy 440-1

Smoke-Free Workplace

Table of Contents

1. Purpose & Background

Establishes policy to provide a smoke-free working environment at BPA facilities.

2. Policy Owner

The Chief Administrative Officer has overall responsibility for this policy.

3. Applicability

This policy applies at all BPA-occupied facilities. At BPA locations other than its Portland headquarters facility, such as the field, the Ross Complex, and Van Mall, on-site management officials or teams develop site-specific procedures using this policy as a guide.

4. Terms & Definitions

Smoking includes use of any smoking material including e-cigarettes and vaping products.

5. Policy

A. Smoking is permitted only in designated areas and only in accordance with the provisions of Executive Order (EO) Number 13058, Protecting Federal Employees and the Public from Exposure to Tobacco Smoke in the Federal Workplace. Smoking, or carrying any lighted smoking material, is not permitted except in designated smoking areas.

B. Employees will not smoke when traveling in any BPA-owned or BPA–leased vehicle.

6. Policy Exceptions

None.

7. Responsibilities

A. **Chief Administrative Officer**: Sets BPA's smoking policy.

B. **Workplace Services and designated senior-level on-site official, or any back-up officials:** Ensure that designated smoking areas are posted and established in a manner that eliminates exposure of employees and the public to secondhand smoke.

C. **Safety Office:**

1. Evaluates, as part of the annual safety inspections, whether smoking areas are properly designated and conform with policy guidelines to provide a safe and healthy work environment for employees.
2. Reports in writing any non-compliance with smoking regulations to the appropriate management official.

8. Standards & Procedures

No information in this section.

9. Performance & Monitoring

As part of its annual safety inspections, the Safety Office evaluates smoking areas for proper designation and conformance to policy guidelines to provide a safe and healthy work environment for employees.

10. Authorities & References

A. 41 Code of Federal Regulations, (CFR), Part 101-20, Smoking Regulations.

B. Executive Order Number 13058, Protecting Federal Employees and the Public from Exposure to Tobacco Smoke in the Federal Workplace.

11. Review

Policy will be reviewed every five years.

12. Revision History

Version Number	Issue Date	Description of Change or Review
1.0	1/25/2017	Initial version in the BPA Policy format. This replaces *BPAM 165 BPA Smoking Policy*.

400/792A.1 PURPOSE This chapter establishes a policy regarding the use and possession of alcoholic beverages, narcotics, and illegal drug substances on BPA property or when in a duty status.

400/792A.2 POLICY The possession and/or use of alcoholic beverages, narcotics, or illegal drug substances on BPA property or when in a duty status is prohibited. Entering on the property while under the influence of alcohol, narcotics, or illegal drug substances is prohibited. Operating a government vehicle at any time or operating any motor vehicle while on the property or in a duty status, while under the influence of alcoholic beverages, narcotics, or illegal drug substances, is prohibited. These prohibitions do not apply in cases where the drug is being used as prescribed for a patient by a licensed physician. However, all rules and regulations concerning operation of BPA vehicles, equipment, aircraft, etc., while using prescribed drugs must be followed. Violation of this policy may result in disciplinary action, up to and including removal.

(Note: While not prohibited under this policy, the use of such substances while off-duty may also lead to disciplinary or other adverse action, depending on the circumstances, e.g., loss of a motor vehicle license by an employee whose job/position requires him or her to have such a license; other off-duty conduct that interferes with the efficiency of the service.)

400/792A.3 RESPONSIBILITIES AND AUTHORITIES

A. The Senior Vice President, Employee and Business Resources (in coordination with the Chief Operating Officer) issues policies related to employee conduct, safety and security, and is designated as the senior management official in charge of the occupational safety and health program

B. Supervisors and managers are responsible for ensuring this policy is followed, and for taking corrective action if the policy is violated.

C. Manager, Personnel Services is responsible for providing advice and assistance to managers with respect to appropriate corrective action.

400/792A.4 REFERENCES

A. Title 41, Code of Federal Regulations, 101-20.307, Alcoholic beverages and narcotics (on GSA property).

B. BPA Manual Chapter 400/792C, Drug-Free Workplace

C. Personnel Letter No. 610-5, Hours of Duty

D. Personnel Letter No. 793-1, Alcohol Testing Implementation Plan

E. The General Services Policy and Procedures Manual Chapter 1023, Conference Room Scheduling and Use

1073.1 PURPOSE To set policy and procedures governing possession, transportation, storage, or use of firearms, other deadly weapons, or explosive devices, on BPA property, in Government vehicles, or in private vehicles located on BPA property or used in the conduct of BPA business or activity. Violation of this policy may result in disciplinary action up to and including removal from the Federal service.

1073.2 DEFINITIONS

A. A firearm is a weapon designed to be held in one or both hands from which a projectile is fired by gunpowder or by other means, and which is designed for and presently capable of causing death or serious physical injury.

B. Deadly Weapon includes any instrument, article or device designed for, and presently capable of, causing death or serious physical injury.

C. Explosive Device includes any fabricated instrument, article or device incorporating explosives and/or incendiary materials and equipped with a fuse or other detonating mechanism, the intention of which is to inflict destruction, property damage, injury, death and/or psychological terror (examples include but are not limited to grenades, fused dynamite, pipe bombs, molotov cocktails, detonators, unexploded military ordnance, etc.). Excluded from this definition is any BPA-owned or contractor-provided explosive used in ongoing construction and maintenance activities.

D. Government Vehicle includes any vehicle or motorized equipment owned, rented or leased by BPA.

E. Government Property includes any equipment, motorized equipment, trailers, motor vehicles, buildings, parts of buildings, sheds, lockers, facilities, or any other physical assets, or any land which BPA owns, rents, leases, or has any real estate rights, interest, or estate. Government property includes any physical asset owned, rented or leased by BPA, whether or not it happens to be assigned to an employee for their use (e.g., motor vehicles, lockers).

F. Private Vehicle includes any vehicle owned, rented, or leased by a BPA employee, a BPA contractor employee, or a member of the general public, which is used primarily for personal use (e.g., getting to and from work) and which is situated on BPA property (or a BPA work site) for any reason whatsoever. Also includes any contractor-owned or -leased commercial vehicles or motorized equipment situated on BPA property (or a BPA work site) for any reason whatsoever.

G. Government Aircraft includes any aircraft owned, rented, leased, or chartered by BPA.

H. Official Duties refers to those activities carried out whenever an employee or contractor is at the assigned BPA post or work, or is in a travel status and actively performing work.

1073.3 POLICY

A. BPA employees, contractors, and the general public are strictly prohibited from possessing, transporting, storing or using firearms, other deadly weapons, or explosive devices

1. While on official BPA duty or on BPA property

2. In Government vehicles

3. In Government aircraft

4. In any private vehicle located on BPA property for any reason

5. In any private vehicle currently being used in conducting BPA business or activities (e.g.,vehicle is situated on a BPA work site or is being used while actively representing BPA to the public)

B. Excluded from this policy are Federal, state and local law enforcement officials, authorized members of the US Armed Forces in uniform, and BPA security and contract security personnel. Also excluded from this policy is the possession, transportation, storage, and/or use of BPA-owned explosives or contractor-provided explosives employed in lawful and appropriate construction and maintenance activities (e.g., blasting tower footings, building foundations and in road construction).

C. The possession, transportation, storage, or use of firearms, other deadly weapons, or explosive devices in privately owned vehicles being used in travel status is discouraged. In this context, "being used in travel status" means using the vehicle to go from home to the hotel/motel, or from the hotel/motel to home - it does not mean going from the hotel/motel to the work site or from the work site to the hotel/motel. Although discouraged, if an employee chooses to do so, the possession, transportation, storage, or use of firearms or other deadly weapons, incident to hunting or other lawful purposes, in private vehicles being used in travel status will be permitted *only* under the following conditions

1. The employee has informed their immediate supervisor

2. If the employee is in travel status (traveling from home to hotel/motel; or from hotel/motel to home) the firearm or other deadly weapon must remain locked inside the vehicle

3. The firearm or other deadly weapon is transported as cargo or luggage

4. The firearm or other deadly weapon is disassembled, if possible

1073.3 POLICY (continued)

5. The firearm or other deadly weapon is at all times enclosed in a carrying case or comparable closed container, whether disassembled or not

6. Under no circumstances shall there be any ammunition in the firearm chamber or magazine

7. While the employee is in travel status, the firearm or other deadly weapon shall be stored at the employee's place of residence or lodging (hotel/motel) and not taken to a job site

D. In addition to the above provisions, carrying of firearms, other deadly weapons, or explosive devices, even as cargo or luggage, is subject at all times to Federal, state, and local laws, ordinances, and regulations.

E. Exceptions. Any and all exceptions to the above policy shall be on a case-by-case basis. Any exception must be specifically authorized in writing by a Tier II Manager with the concurrence of the Manager for Security Services.

1073.4 RESPONSIBILITIES

A. The Senior Vice President for Business Services issues policies related to employee safety and security.

B. Tier II Managers review and approve/disapprove employee requests for exceptions to this policy in coordination with the Manager for Security Services.

C. The BPA Manager for Security Services concurs with the Tier II Manager's recommendation authorizing exceptions to this policy.

1073.5 PROCEDURES FOR EXCEPTIONS

A. Employee submits a written request through their first level supervisor to his or her *Tier II Manager*, requesting an exception to this policy. The written request shall fully describe the underlying circumstances and rationale for the exception.

B. Tier II Manager reviews the request for an exception and determines whether it complies with the intent of this policy. Assures that the employee understands any and all conditions affecting the exception. If the Tier II Manager approves the request for an exception, they then authorize the exception in writing, after consulting with and obtaining the concurrence (in writing) of the Manager for Security Services.

1073.6 REFERENCES

A. Title 18, US Code, Section 930, Possession of Firearms and Dangerous Weapons in Federal Facilities.

B. Code of Federal Regulations, 41 CFR 101-20.313, Federal Property Management Regulations, Weapons and Explosives.

C. *BPA Personal Property Manual*, Volume IV, Chapter 1, pp. 1.7 and 1.7a.

D. *BPA Manual* Chapter 180, Safety and Health Program.

3.2 STANDARDS OF CONDUCT REGARDING INDEPENDENT FUNCTIONING AND TRANSMISSION INFORMATION

3.2.1 General

(a) The Standards of Conduct (SOC) promulgated by the Federal Energy Regulatory Commission through Order No. 717 apply to public utilities as defined by Section 201(e) of the Federal Power Act. Bonneville is not a public utility but has elected to comply with these rules to the extent possible consistent with its statutory responsibilities.

(b) One of the tenets of the SOC is the Independent Functioning requirement. The purpose of Independent Functioning is to prevent the marketing function of a Transmission Provider from gaining a competitive advantage over non-affiliated customers or potential customers of the Transmission Provider. The marketing function within Bonneville now resides with employees involved in the sale of energy or capacity. They are required to have limited interaction with the personnel within Transmission Services that operate the transmission system on a day-to-day basis.

3.2.2 Policy

It is Bonneville's policy that employees and contractors engaged in all phases of purchasing and contract administration comply with SOC as described above.

3.2.3 Procedure

COs shall contact the SOC Compliance Officer at SOC@bpa.gov to address any concerns or questions regarding SOC. Requisitioners, CORs and Field Inspectors shall contact both the CO and the SOC Compliance Officer to address and resolve SOC issues.

TITLE: Personal Identity Verification and Personnel Risk Assessment Policy and Procedures for Issuance of Access Privileges and Credentials

AUTHOR: Kirsten Kler/Launie O'Leary (Final after Union negotiations on Sept 11, 2009; updated March 2010 to support NERC CIP Version 2 changes); undergoing revision in support of NERC CIP v4 June 2012

DATE: Revised January 2013 (previous versions dated March 2010, September 2009, June 2008)

APPROVAL AUTHORITY: Christina J. Munro, Chief Security Officer, Office of Security and Continuity of Operations, Bonneville Power Administration for Kirsten M. Kler, Acting 1/31/2013

POLICY:

The Office of Security and Continuity of Operations (OSCO) is the responsible organization for implementing the requirements of Homeland Security Presidential Directive-12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors; DOE Notice 206.4, Personal Identity Verification (PIV); and the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection Standard (CIP) 004-3 R3 pertaining to initial and recurring Personnel Risk Assessments (PRA) for personnel authorized unescorted physical and logical access to BPA facilities that contain critical cyber assets. OSCO will ensure that all employees (federal and contractor workers) who require unescorted physical access to BPA facilities and/or require logical access (IT account), will undergo required personal identity verification and NERC-CIP required Personnel Risk Assessments , as described in this policy. All employees (federal and contractor) who successfully complete an initial personnel investigation and identity verification process will receive a BPA identification badge with electronic physical access to areas that have been approved. Under no circumstances shall any person have unescorted physical or logical access to any assets until the individual has successfully completed the PIV process, received a favorable criminal background investigation, and been issued a Smart Credential or local site specific only badge (LSSO). Exceptions to this policy are allowable only in support of emergency situations. OSCO's Personnel Security Office shall serve as the agency's official source of record of verification of an individual's authorized issuance of physical and logical access rights in accordance with the successful completion of PIV and NERC CIP requirements.

APPLICABILITY:

This policy and the following security procedures apply to all current and potential federal employees and contractor workers of the Bonneville Power Administration.

REQUIREMENTS:

A. OSCO shall establish local policies and procedures in support of DOE's responsibilities for identity, credential, and access management as described in DOE Order 206.2 and DOE Order 473.3:

1. Provide a trusted framework and common identity infrastructure for access to BPA/DOE facilities and systems;
2. Supports the management of federated identity records from trusted identity providers both within and outside the Federal Government;
3. Shall subscribe to Privilege Management concepts whereas BPA Employees and contract workers will have access to information systems and facilities to which they are entitled and only for the time period or duration which they require it.

4. Issue ID badges only to individuals whose identity has been verified by two source identity documents.
5. Prescribe local procedures for issuance, use, accountability, and return of ID badges.
6. Complete the appropriate level of personnel investigations going back at least 7 years.
7. Establish and follow processes and procedures for revoking or confiscating expired or invalidated ID badges.
8. Issue only approved security ID badges as outlined in DOE Order 473.3, Attachment 3, Section A, Chapter XI, DOE Security Badge, Credential and Shield Program.
9. Ensure that foreign nationals are processed in accordance with DOE O 142.3 prior to physical access and identification badge issuance.
10. Develop clear documentation on the rules of behavior and consequences for failure to comply before granting physical access to facilities and/or systems.
11. Ensure that responsible personnel (Personnel Security Specialists) understand their responsibilities for implementing PIV policy and issuing physical access.
12. Responsible for ensuring that all personal information collected for employee and contractor identification is handled in accordance with approved Systems of Record notifications.

B. OSCO provides support to Human Capital Management in ensuring NERC CIP compliance for standard CIP-004-3 R3, Personnel Risk Assessments. OSCO shall:

1. Ensure the appropriate initial criminal background investigation and personnel risk assessment is performed on all persons that require unescorted physical access to BPA facilities that contain critical cyber assets per NERC-CIP-004-3 R3;
2. Ensure that federal employees and contract workers subject to the requirements of a recurring criminal background investigation and identity verification (per NERC-CIP-4-3 R3) will complete these actions every 7 years. In addition, recurring criminal background checks may be conducted at any time for cause (for purposes of this issuance, BPA defines "cause" as facts that reasonably call into question the continued appropriateness of an employee's ability to either work directly with critical cyber assets or enter a facility that contains critical cyber assets on an unescorted access basis);
3. Conduct a periodic review of records verify access to critical cyber assets that OSCO manages was authorized upon successful completion of NERC CIP PRA requirements. Reviews will be documented and maintained on site.

RESPONSIBILITIES:

A. **Applicant and/or Existing Employee/Contract Worker** – Responsible to complete required forms; provide fingerprints, and source identity documents as requested during the initial PIV process or recurring 7 year PRA investigation; is responsible for arriving for all scheduled appointments on time; shall safeguard badge against loss, theft, or misuse; shall report to Security when the badge is lost, stolen, or misused within 24 hours of discovery; shall maintain the Smart Credential/badge in good condition and protect its integrity by ensuring that the badge is not altered, photocopied, counterfeited, reproduced, or photographed; assumes the cost for fingerprinting when fingerprinting cannot be completed at BPA Headquarters, Portland, OR (exception for existing federal employees employed at BPA will be reimbursed, for any fingerprinting fees incurred, upon submittal of BPA Form 2230.06e Claim for Reimbursement for Expenditures to Finance, with costs charged to the following: Dept ID: NNP; ABM: LRAC; Bus. Unit: CORPT; Work Order: 00257172; Task: 04; GL Account: 600420; DCE: OEB). If a Smart

Credential will be issued, the applicant/employee is responsible for scheduling/cancelling enrollment and activation appointments and for completing all appointments on time.

B. **Chief Human Capital Officer (CHCO)** – Responsible to ensure personal identity has been verified and receipt of a favorable criminal history check based on fingerprint results prior to officially offering a position of employment to a federal applicant. Responsible for ensuring completion of Non-Government Employee Data is entered into the Human Resources Management Information System (HRMIS) via the BPA Form 1400.22e for contract applicants. Responsible for ensuring that vacancy announcements note the risk assessment category of the position (including at a minimum Position Sensitivity Codes, Risk Designations, and Security Clearance Levels) along with required risk assessment procedures for each category. Ensure that all federal positions have a position sensitivity risk designation and HCM staff members communicate the required type of background investigation a new hire into a federal position is required to complete.

C. **Chief Information Officer (CIO)** – Responsible to ensure an individual's personal identity has been verified and receipt of a favorable criminal history check based on fingerprint results prior to authorizing logical access to any BPA government system.

D. **Chief, Office of Security and Continuity of Operations (OSCO)** – Responsible for program oversight and implementation of HSPD-12 and DOE Notice 206.4; providing support to Human Capital Management in ensuring compliance under the NERC CIP standard CIP-004-3 R3; and appointing, in writing, staff to fulfill the roles of Registrar, Adjudicator, Security Officer, Enroller/Activator, Sponsor, Issuer, and Registrar by Proxy.

E. **Contracting Officer's Technical Representative (COTR)** - Responsible for ensuring the contractor applicant has all required forms necessary to initiate the initial PIV screening process, coordinates with the Sponsor for Smart Credential enrollment, facilitates the transfer of completed paperwork (forms) from the applicant to Personnel Security, NNP-B1; reviews all applicable forms for completeness prior to sending to NNP-B1; shall respond in a timely manner to NNP-B1 to resolve any issues involving the applicant that may arise during the PIV process; Responsible for safeguarding all sensitive information for the protection of the applicant's privacy, and must comply fully with applicable federal laws and agency directives to include: The Privacy Act of 1974, E-Government Act of 2002, OMB M-03-22, FIPS 201. COTR must be a federal employee.

F. **Field Registrar Designee** - An employee who performs limited functions such as verifying I-9 documents, as designated by the registrar. Registrar Designees are not permitted to fingerprint applicants, and are assigned and designated by the Personnel Security Registrar. Field Registrar Designee may be a federal or contractor worker.

G. **HCM Suitability Adjudicator** – Delegated by the Chief Human Capital Officer (CHCO). The HCM Suitability Adjudicator is responsible for: reviewing the personnel investigation and/or Special Agency Check (SAC) reports for federal employees for a determination on employment suitability or other appropriate administrative action; documenting such determinations and safeguarding records in accordance with applicable laws and regulations; and completing any required actions for employees for whom adverse information is received that results in a determination that the employee is either unsuitable for continued federal employment or other administrative action. HCM Suitability Adjudicator must be a federal employee. In exercising these responsibilities, HCM will adhere to the provisions of PL-731-1.

H. **Issuer** - Responsible for physical issuance of the Local Site Specific Only (LSSO) badge and BPA physical access proximity card (BPAC). Issuer responsible for importing data elements from the employee's Smart Credential into BPA's electronic Physical Access Control System (PACS) for physical access issuance purposes. Issuer will not issue physical access rights without the approval of the Security Adjudicator; responsible for safeguarding all sensitive information and for the protection of the applicant's privacy and must comply fully with applicable federal laws and agency directives to include: The Privacy Act of 1974, E-Government Act of 2002, OMB M-03-22, DOE N 206.4, and FIPS 201. Issuer may be a federal or contract worker, and is part of the OSCO office.

I. **Personnel Security Registrar** – Completes the Electronic Questionnaires for Investigations Processing (e-QIP) for all new applicants. Collects all required forms in support of the overall PIV process. Collects all required identity source documents. Responsible for requesting file release requests from OPM on previously conducted background investigations, release fingerprints to OPM for criminal history checks (CHC), and submits eQIPs to OPM to initiate background investigations. The Personnel Security Registrar must be a federal employee.

J. **Personnel Security Registrar Designee** – Responsible for review and processing of PIV and eQIP forms in preparation of criminal history checks and background investigations. Creates and updates PIV Files and databases, and schedules and conducts PIV appointments. The Personnel Security Registrar Designee may be a federal or contract worker.

K. **Personnel Security Adjudicator** - Responsible for reviewing the OPM/FBI results for both fingerprint check and personnel investigation for federal employees and contract workers undergoing their initial or subsequent investigation for a determination on physical access suitability; determines if results are either favorable or unfavorable based on adjudication guidelines issued by OPM and DOE; documents determination and appropriately records results in approved systems; For unfavorable determinations, shall notify Supervisor, PERSEC; provides fingerprint and personnel investigation results to the Human Capital Management office for all federal employees who will then make final Suitability Adjudication; safeguards all sensitive, personal information and ensures compliance with all applicable federal laws and agency directives to include: The Privacy Act of 1974, E-Government Act of 2002, OMB M-03-22, DOE N 206.4, and FIPS 201. Security Adjudicator must be a federal employee.

L. **Registrar by Proxy (Field Registrars)** - An employee who fulfills limited registrar duties in a designated area. BPA Registrar's by Proxy perform a limited number of Registrar duties to include fingerprinting and identity verification. Registrar by Proxy or Field Registrar must be a federal employee.

M. **Sponsor** - The sponsor initiates the process for an applicant to enroll for a Smart Credential and as such bears the responsibility for justifying the agency's cost of submitting an individual for a background investigation and identity verification. If the applicant does not yet exist in the system, the Sponsor creates a New Applicant Record. The Sponsor updates the employee status (Active/Suspended/Terminated) in US Access for assigned employee/contract workers as their employment status with BPA changes. Sponsor maintains knowledge of responsibilities and shall stay current on US Access updates; Ensures accurate data is entered into US Access to minimize undue cost to the agency for invalid records; responsible to safeguard all Personally Identifiable Information (PII), and for the protection of the applicant's privacy and must comply fully with

applicable federal laws and agency directives to include: The Privacy Act of 1974, E-Government Act of 2002, OMB M-03-22, FIPS 201. The Sponsor must be a federal employee.

N. **US Access Registrar** - Responsible for collecting and entering all required information on the new employee (federal or contractor) for enrollment of a Smart Credential into the Identity Management System (IDMS) by collecting personal information, scanning identity documents, taking fingerprints and photo. Also assists employees with Smart Credential activation process. Enroller/Activator may be a federal or contract employee, and is part of the OSCO office Responsible for managing the schedule, conducting enrollment/activation appointments, verify sponsorship information in the Identity Management System (IDMS), verify and scan applicant identity documents, capture applicants photo and fingerprints, and flag any issues during enrollment.

PROCEDURES:

The procedures for granting physical access vary based on the nature of the request, the level of oversight that will be enforced, and the anticipated duration of access. The specific procedures, described below, address each situation. Managers/COTRs/Sponsors must determine an applicant's physical access requirements and request the appropriate type of physical access. Prospective federal and contract workers must successfully complete the appropriate initial OPM background investigation or criminal history check prior to issuance of any type of physical access privileges. Sections A1 through A3 below refer to requirements and procedures for prospective new employees (federal and contractor workers). Section A6 below addresses procedures and requirements that apply solely to existing employees (federal and contractor) who are subject to NERC CIP PRA requirements.

A. Physical Access:

1. Types of physical access:

a. Temporary Escorted Access: Joint approval by Personnel and Physical Security is required to authorize temporary escorted access. Persons authorized temporary escorted access are: performing work for a period less than 6 months, do not require any type of logical access to perform work, shall be escorted at all times during performance of work while on site. All persons authorized temporary escorted access must successfully complete identity verification. This can be accomplished by BPA staff or by the contract company in accordance with identified procedures. Persons granted temporary escorted accesses are required to check in/out at the designated entry point, or as described in the contract.

b. Unescorted Physical Access: This type of physical access is for contract workers performing work at BPA facilities/sites for a period up to 5 years. Unescorted physical access does not include BPA logical access. Some examples of contract worker types requiring unescorted physical access would be janitorial staff, landscape personnel, and facilities maintenance staff. Persons authorized unescorted physical access shall successfully complete identity verification and a national criminal history check. Upon favorable adjudication of the individual's criminal history, the contractor shall be issued a LSSO with expiration not to exceed 5 years from the date of issue.

c. Unescorted Physical and Logical Access: This type of access is for routine federal and contract workers that require unescorted physical access and logical access to perform work, regardless of duration of work performance period. Persons authorized physical and logical access shall complete

identity verification and, at a minimum, a National Agency Check with Inquiries (NACI) OPM investigation.

First, BPA will submit documents to OPM and request an appropriate personnel investigation. Second, due to the potential that the response timeframe of this request will impact the start date of the new employee, Bonneville will accept a favorably adjudicated fingerprint result and will issue a BPA Local Site Specific Only (LSSO) Badge or a Provisional PIV Credential (Smart Credential). The provisional PIV Credential (Smart Credential) will only be issued if the investigation results have not been received within five working days after the receipt of fingerprint results. Favorable fingerprint results will authorize the applicant cyber/logical access.

	Temporary Escorted Physical Access	Unescorted Physical Access	Unescorted Physical and Logical Access
Contractor	X	X	X
Vendor	X	X	
Consultant		X	X
Off site worker*	X		X
Federal employee			X
Volunteer**		X	X
Student			X
NERC CIP CCA		X	X
Project Wise***		X	

*Off Site worker – a contractor that works remotely and typically either occasionally needs to come on site to attend meetings or provide work products, or may be performing work that would require logical access to remote systems or FTP exchanges. If logical access is needed, the offsite worker is required to complete the Physical and Logical Access requirements.
**Volunteer – volunteers may or may not require cyber access. If they in fact require cyber access, they will be required to complete the Physical and Logical Access requirements.
***Project Wise – offsite workers requiring access to ProjectWise are required to complete the Unescorted Physical Access process.

	Temporary Escorted Physical Access	Unescorted Physical Access	Physical and Logical Access (includes CCAs) (CFTE)	Physical and Logical Access (Includes CCAs) (BFTE)
Identity Verification	X	X	X	X
Photo		X	X	X
Fingerprints		X	X	X
Criminal History Check (SAC only)		X		
NACI			X*	X*
Public Trust			X**	X**
Clearance				X***

*NACI required for Physical and Cyber Access privileges and will result in issuance of Smart Credential.
**Some positions are designated as Public Trust and the incumbent of that position must undergo a higher background investigation to include credit history. This kind of check will result in issuance of a Smart Credential.
***A very small number of federal positions are designated as having access to national security information. Incumbents of those positions must undergo a higher background investigation which will assess character, loyalty, credit and criminal history, education, residences and reference checks. This check will result in issuance of an L or Q clearance which will be noted on the individual's Smart Credential.

2. Processing Requirements:

Once the potential federal employee or contract worker (also known as the "applicant") is tentatively selected, they must fully complete required identity verification and Smart Credential actions and appointments. HCM Representatives, Sponsors and COTRs shall work closely with Personnel Security staff to ensure all required forms and appointments are completed accurately and in a timely.

a. Initiating the Personnel Identity Verification (PIV) Process:

1) To initiate the PIV process for federal and contract workers the HCM Representative or COTR is responsible for submitting the PIV Request via Entrust encryption e-mail or through internal BPA mail
    a. Contract Worker requests must be submitted using BPA form 5632.19e.
    b. Federal employee requests must be submitted using BPA form 5632.26e.
2) The HCM Representative or COTR is responsible for reviewing all required forms for completeness and accuracy prior to sending the originals to Personnel Security.
3) The HCM Representative or COTR is responsible for creating a correlating entry in Service Connection prior to submitting the PIV Request form to Personnel Security.
    a. Personnel Security staff will not begin PIV actions until a Service Connection entry is recorded.
    b. Personnel Security staff will remind COTRS and HCM Representatives if a Service Connection entry is missing.
4) The HCM Representative or COTR ensures the federal/contract worker is sponsored in US Access. If the HCM Representative or COTR is not aware of whom their USAccess Sponsor is they can send an e-mail to the "Smart Card Help" e-mail box for assistance.
5) Contract Workers require two additional forms be submitted at the time of PIV request:
    a. The Supplemental Notice to Contract Employees Form 5632.28e must be completed and sent along with the PIV Request.
    b. Non-Government Data in HRMIS Form 1400.22e must also be completed, but is sent to Non-Government Employee Processing, NHO-1 only.

b. Smart Credential Enrollment/PIV Appointment and Release of Fingerprints to OPM:

1) Once the PIV request is received by Personnel Security, the federal/contract worker will be contacted to schedule appointments.
2) The applicant must bring two forms of unexpired identification to the Smart Credential Enrollment and/or PIV appointment. At the appointment the employee or contract worker's identity documents will be validated, fingerprints captured, and a photograph taken.
3) Upon completion of the Smart Credential Enrollment and/or PIV appointment the fingerprints that were captured during the appointment are released to OPM to begin processing of the Criminal History Check.
    a. Criminal History Checks with OPM take from 3-5 days to receive results.
    b. Results indicating a "record" will require additional review which can take approximately 7-14 additional days to process.

c. Actions upon return of the Criminal History Check Favorable Results:

1) Upon favorable adjudication of the Criminal History Check and receipt of all required forms, the federal employee or contract worker will be "Cleared for Badging" and an e-mail notification will be sent to the HCM Representative/COTR, USAccess Sponsor, RAMS Security, and Badging/Access Issuer.
2) Personnel Security will submit all forms and eQIP documents to OPM to begin processing of the NACI investigation at this time.
3) Personnel Security will issue a BPA LSSO or Provisional PIV Credential (Smart Credential) to the approved federal employee/contract worker.
4) The Cyber Security Office will issue cyber access privileges in accordance with Cyber Security policies.
5) Contract Workers shall not begin performing work in advance of the "Cleared for Badging" notification.
    a. Specific, unique requests can be submitted in writing to the Manager for Personnel and Information Security.
    b. COTRS, Sponsors and Managers are not allowed to use the BPA Visitors Form in lieu of the "Cleared for Badging" notification. That is misuse of the Visitors Form and considered a circumvention of policy.

d. Actions upon return of the Criminal History Check Unfavorable Results:

1) Upon unfavorable adjudication of the Criminal History Check, the Personnel Security Adjudicator may send out a Letter of Inquiry to the employee or contract worker if further clarification or elaboration is needed to aid in the determination on the access credential eligibility. (For disqualifying criteria, see section 3 below)
2) If deemed ineligible to hold a BPA access credential the Personnel Security Adjudicator may send the employee or contract worker and the HCM Representative/COTR a letter denying the issuance of a BPA Security Badge or Smart Credential. The employee or contract worker is given the right to appeal. (For appeal rights, see section 4 below)

e. Actions upon return of complete NACI Investigation with Favorable Results:

Upon favorable adjudication of the NACI investigation results the Personnel Security Office will complete the PIV File. The HCM Representative or COTR will not be notified that the investigation is now fully complete.

f. Actions upon return of complete NACI Investigation with Unfavorable Results:

1) In the case of a federal employee whose complete NACI investigation results indicate non-approval HCM will adjudicate and make final determination for employment suitability. Appeal rights are described in section 4 below (PIV) and 731-1 (Suitability).
2) In the case of a contract worker whose complete investigation results indicate unfavorable, the Personnel Security Adjudicator may send out a Letter of Inquiry to gather more information on the case. If the applicant clearly falsified information, the Adjudicator may send the contract worker and COTR a letter withdrawing the issuance of a BPA Security Badge or Smart Credential. If the credential issuance is withdrawn, the applicant is given the right to appeal. If the appeal is denied, the COTR will work with the contracting firm to pursue another contractor candidate. (For disqualifying criteria, see 3 below)

3. Denial of Issuance of Physical and/or Cyber Access or Smart Card:

When the personnel investigation, or any part thereof, including the FBI criminal history fingerprint portion is received, it, or a copy, will be forwarded to the designated Adjudicator for adjudication. Adjudication includes both Security adjudication and Suitability Adjudication. In the adjudication process, the adjudicator shall have the authority to obtain additional information as may be deemed necessary to resolve possible issues of concern pertaining to the applicant.

The following are disqualifying criteria, but are not all inclusive, and may vary depending on the position that the contractor worker or federal employee will hold:

a. The FBI determines the individual is, or is suspected of being, a terrorist.
b. There is an outstanding warrant against the individual.
c. The individual has deliberately omitted, concealed, or falsified relevant and material facts from any *Questionnaire for National Security Positions* (SF 86), *Questionnaire for Non-Sensitive Positions* (SF 85), OF306 Declaration for Federal Employment (Including federal Contract Employment), or similar form used in the determination of eligibility for a DOE security badge.
d. The individual has presented false or forged identity source documents.
e. The individual has been barred from federal employment.
f. The individual is currently awaiting a hearing or trial, has been convicted of a crime punishable by imprisonment of six months or longer, or is awaiting or serving a form of pre-prosecution probation, suspended or deferred sentencing, probation, or parole in conjunction with an arrest or deferred sentencing probation, or parole in conjunction with an arrest or criminal charges against the individual.

4. Appeals Process Regarding Denial of badge or Smart Credential:

- **a.** For unfavorable adjudication under the criteria in paragraph 3 above, the adjudicator must do the following within 2 working days of the determination: a) notify the sponsor in writing that a BPA security badge will not be issued to the applicant and b) notify the applicant in writing of the unfavorable adjudication (the notification must contain the reasons for the denial of the BPA security badge and appeal process available).If the federal or contractor applicant has been denied the issuance of a BPA Security Badge or Smart Credential, he/she have the right to appeal the decision. Upon receipt of the adjudicator's denial of badge/credential notice, the applicant has 10 working days in which to indicate in writing or by electronic means the intent to file an appeal. The applicant must file the actual appeal within 10 working days after notification of intent to file. The appeal must be in writing and provide a response to the information that formed the basis of the denial of security badge or Smart Credential.
- **b.** The applicant may be represented and advised by counsel or a representative of his/her choosing in the appeals process at his/her own expense. The applicant's counsel may provide written documents to support the case, but neither the applicant nor counsel will be present during the Appeals Panel.
- **c.** The Adjudicator will identify and notify members of the appeals panel who must be federal BPA employees. The panel consists of one "Q" (Top Secret) cleared security office representative, one uncleared General Counsel representative and one uncleared representative from the department or field element having cognizance over the site. The appeals board reviews the applicant's appeal and adjudication information and decides whether the applicant will be issued a badge or credential. The decision is made by majority of concurrence or nonconcurrence and the decision is final.
- **d.** The applicant will be notified in writing of the appeals panel decision. The applicant can share this with anyone he/she chooses as a representative.

NOTE: DOE Notice 206.4, Personal Identity Verification (PIV), requires three Q (Top Secret) cleared members for the Appeals Board; however, BPA has an approved deviation from this policy dated February 2, 2007, stating that a BPA appeals panel can consist of one Security "Q" Cleared employee, a non-cleared general counsel employee, and a non-cleared field element representative with cognizance over the site.

5. Records and Documentation:

- **a.** At least annually, Personnel Security staff shall conduct a random audit of 10% of its badged population to assess access badges or Smart Credentials were issued only to persons that completed the PIV process, and have a favorable background investigation on file.
- **b.** These reviews will be documented, discrepancies identified and reconciled, corrective actions noted.
- **c.** All documentation shall be maintained for at least 12 months, or until superseded by an updated records review.

6. NERC-Required Personnel Risk Assessments:

- **a.** In accordance with NERC CIP-004 R3, Personnel and Training, employees (federal and contractor) with unescorted physical access to facilities with critical cyber assets are required to

undergo recurring criminal background check and identity verification every 7 years. The following describes the actions BPA organizations will complete to meet this NERC CIP requirement:

1. OSCO will track, in partnership with HCM, all individuals with authorized access to CCAs. At 6 months prior to expiration, employee will be contacted to commence reinvestigation and identity verification. At this time an assessment of the employee's ongoing need for access will be completed and verified. Once confirmation of continued need to access is received, employee will be scheduled to provide fingerprints and complete identity verification process. Fingerprints will be submitted to OPM for a SAC nation-wide criminal history check for the last 7 years.

2. OSCO shall track contractor wrokers with access to CCAs. Those contractors with continued need for access to CCA's shall be contacted 6 months prior to expiration and initiated for a reinvestigation. Reinvestigation shall include identity verification and collection of fingerprints to be sent to OPM for a SAC nation-wide criminal history check.
3. For federal and contractor workers undergoing PRA reinvestigations for NERC CIP compliance, all results from reinvestigations shall be adjudicated, results documented and recorded in appropriate systems, and available for inspections as needed.

b. In accordance with NERC CIP-004-3, Personnel and Training, management may require employees (federal and contractor) to undergo a criminal background check at any time for cause ("cause" is defined as facts that reasonably call into question the continued appropriateness of an employee's ability to either work directly with critical cyber assets or enter a facility that contains critical cyber assets on an unescorted access basis). To initiate such a check, line management works with the HCM Suitability adjudicator (or the CO/COTR in the case of a contractor worker), presenting the reasoning. HCM (or the CO/COTR in the case of a contractor worker) will advise the employee of the requirement and the reasons for the check, along with their appeal rights. HCM (or the CO/COTR in the case of a contractor worker) will advise SER, which will then initiate action to have the employee undergo the criminal background check (fingerprint only).

c. HCM will review and adjudicate the fingerprint reports for federal employees to determine ongoing employment suitability or other administrative action, as appropriate (e.g., retention in federal service may be determined to be appropriate but not in a position that works with critical cyber assets or that requires access to facilities that contain critical cyber assets).

1. All adjudications of Personnel Risk Assessment results by HCM will be based on the same criteria included in PL No. 731-1, Suitability Determinations, notwithstanding the fact the determination may result in an administrative action other than removal from federal service, as appropriate.
2. Employees whose adjudications result in determination for either removal from continued federal service or other administrative action will be notified in writing in accordance with applicable regulations. Such employees will be covered by MSPB appeals rights (as applicable) or either negotiated grievance procedures or the administrative grievance procedure if they choose to contest the action (see PL No. 752-1 for more information regarding MSPB appeal rights).

d. OSCO and HCM designated staff shall review and adjudicate the personnel investigation reports for all contractor workers to determine ongoing physical access eligibility.

1. Staff shall utilize published adjudication guidance issued by OPM and DOE; and
2. Staff shall notify the contractor worker and the responsible COTR or Sponsor on any unfavorable determinations.
3. Contractor workers with unfavorable background investigations may be denied further/ future physical access to BPA facilities.

e. BPA shall provide training in accordance with NERC CIP-004-3. Management shall provide a point of contact for employees who have questions about the process. The point of contact shall be an employee who is knowledgeable about NERC personnel risk assessment requirements/standards.

7. **Release of Information:** When a subject of investigation asks for a copy of his/her own investigative file, he/she should be advised that OPM provides a copy of the file under a Privacy Act request. The individual must make a written request for the file to OPM-FIPC, FOI/PS, PO Box 618, Boyers, PA 16018-0618. The request must include the full name, AKA's, SSN, DOB, POB, full address, and location of present or former Federal employment and it must be signed by the requestor.

REFERENCES:

A. Homeland Security Presidential Directive 12 - Policy for a Common Identification Standard for Federal Employees and Contractors, dated August 27, 2004. http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html.

B. Federal Information Processing Standards Publication 201-1, Revised Standard for Personal Identity Verification of Federal Employees and Contractors, dated March 14, 2006. http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-v5.pdf.

C. DOE Notice 206.4 - Personal Identity Verification, dated June 29, 2007. http://www.directives.doe.gov/cgi-bin/explhcgi?qry1735846358;doe-77.

D. Personnel Letter No. 731-1, Suitability Determinations, dated June 25, 2008.

E. Personnel Letter No. 752-1, Discipline, Adverse Actions, and Alternative Discipline, dated August 29, 2003.

F. North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection Standard CIP-004 Personnel and Training, version 3 and 4.

BPA Policy 433-1

Information Security

Table of Contents

1. Purpose & Background

This policy sets forth Bonneville Power Administration's (BPA) Information Security Program for Controlled Unclassified Information (CUI), and outlines guidelines for identifying, handling, and controlling CUI. BPA identifies three categories of CUI: Official Use Only (OUO) Information, Bulk Electric System Cyber System Information (BES CSI), and Critical Information. This policy and accompanying procedures for each information type specify requirements for security controls when information is in storage, transit or use.

BPA's Information Security Program also includes Classified Information, which is identified and controlled for the purposes of national security. BPA employees with classified security clearances are authorized by the Department of Energy to handle that information. A separate set of procedures address Classified Information at BPA and are not reflected in this policy.

2. Policy Owner

The Chief Administrative Officer is the owner of this policy.

3. Applicability

This policy applies to all Bonneville Power Administration employees.

4. Terms & Definitions

A. **BES Cyber System Information (BES CSI)**: Information about Bulk Electric System (BES) Cyber Systems that could be used to gain unauthorized access or pose a security threat to BES Cyber Systems.

Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that are not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System. (NERC Glossary of Terms Used in NERC Reliability Standards – Updated 7/7/2014).

BES Cyber System Information was formerly known as Critical Cyber Asset Information (CCAI).

B. **Controlled Unclassified Information (CUI)**: Information required by laws, regulations, or government-wide policies to have security controls (excluding classified information). BPA identifies three types of CUI: Official Use Only, Bulk Electric System Cyber System Information, and Critical Information.

C. **Critical Information**: Information that requires Operational Security (OPSEC) measures because it reveals an operational vulnerability. Defined as "specific facts about friendly (e.g., U.S.) intentions, capabilities, or activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for accomplishment of friendly objectives" (DOE O 471.6).

D. **Critical Information List (CIL)**: A list identifying BPA's CUI by organization/function and by category — OUO, BES CSI, or other Critical Information.

E. **Federal Record**: All recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them. Materials made or acquired solely for reference, extra copies of documents preserved only for convenience of reference and stocks of publications are not included. See Federal Records Act, 44 USC §3301.

F. **North American Electric Reliability Corporation-Critical Infrastructure Protection (NERC CIP)**: A body of regulatory compliance standards and requirements related to the protection of bulk electric system cyber and physical assets.

G. **Official Use Only (OUO)**: A category of CUI that requires security controls. OUO is identified by these characteristics:

1. Information has the potential to damage governmental, commercial, or private interests if released to those who do not need the information to perform their jobs at BPA or to perform other BPA authorized activities, AND

2. Information that may be exempt from public release under the Freedom of Information Act (exemptions 2-9). For more information about the FOIA exemptions, see section 8 below.

Note: BPA's FOIA Officer makes the final decision on release of all agency records under FOIA, including the release of records that were previously designated as OUO.

5. Policy

To ensure the continued reliability of the power grid and comply with Federal and industry standards, BPA categorizes, safeguards, and controls information. BPA employees protect information from unauthorized access in order to safeguard people, operations, and assets. To ensure adequate security controls are implemented, BPA personnel must use the following steps:

A. **Identify**: Determine if the information created or received qualifies as Official Use Only (OUO), Bulk Electric System Cyber System Information, Critical Information, or

unclassified, depending on thresholds (see Procedures section below). If so, follow steps B-E.

B. **Mark**: Clearly mark information according to specific standards for each CUI category.

C. **Control**: Ensure that protection requirements are in place and upheld throughout the lifecycle of the information, from creation to destruction, regardless of form. Information must be shared, handled, and stored according to procedures specified for its CUI category.

D. **Destroy**: Copies of controlled information must be destroyed when no longer needed. Federal Records containing controlled information must be maintained according to the retention schedule determined by the Agency File Plan and in compliance with security control requirements.

E. **Report**: Loss, misuse or mistreatment of information is reported to InformationProtection@bpa.gov.

6. Policy Exceptions

There are no exceptions to this policy.

7. Responsibilities

A. **The Chief Administrative Officer**: Ensures effective safeguards, security policies and programs are in place at BPA to prevent unacceptable and adverse impacts on national security, the safety of BPA personnel, the public, and the environment.

B. **The Chief Security and Continuity Officer**: Ensures implementation and compliance with DOE Order 471.3, DOE Order 471.6 and NERC CIP 011-2 R1. The CSCO directly or by delegation ensures that the program contains the following elements:

1. Identification and protection of Classified Information.
2. Identification and protection of Official Use Only Information.
3. Identification and protection of BES Cyber System Information.
4. Identification and protection of Critical Information.
5. Adherence to BPA Self-Assessment Program.
6. Development and delivery of the BPA Training and Awareness Program.
7. Coordination with the CIO and NERC CIP Senior Manager on matters related to information protection.

C. **The Chief Information Officer (CIO)**: Supports and assists the Chief Security and Continuity Officer in safeguarding BPA's classified and controlled unclassified

information. The CIO has delegated this responsibility to the Chief Information Security Officer (CISO) as the senior agency information security officer.

D. **The Chief Information Security Officer**: Is responsible for the following relative to the delegation of the CIO:

1. Develops and maintains the agency Cyber Security Program (CSP) and works with the Chief Technology Officer (CTO) regarding the standards documentation and supporting governance.
2. Establishes and maintains an office to manage the agency CSP that implements information security requirements while reserving the capability for independence in reporting in accordance with the CSP.
3. Effectively collaborates with and supports the Grid Operations Information System Security manager for implementation of the Cyber Security Program Plan (CSPP) for Transmission, and provides support pursuant to the Federal Energy Regulatory Commission orders or requirements related to cyber security.
4. Identifies cyber assets that may require specific additional Security Plans under the agency CSP.
5. Assists the Operations Security Working Group representatives and Agency Vice Presidents with cyber security issues related to the electronic management and safeguarding of OUO and BES CSI information.
6. Ensures training and appropriate oversight of personnel with significant responsibilities for information security and information technology.

E. **The FOIA Officer**: Works in consultation with the Office of General Counsel to determine when the FOIA requires release of information previously designated as OUO.

F. **Organizational Managers**: Participate in performance and monitoring activities as directed by the Office of Information Security, including the annual assessment of adherence.

G. **BPA employees**: Complete the Information Protection training within thirty days of hire, and annually thereafter.

8. Standards & Procedures

Procedural documents accompanying this policy give specific instructions for the handling of each category of Controlled Unclassified Information, from creation to destruction. The following describes how to identify each category. Once identified, refer to BPA Procedures for handling instructions.

A. **Identifying Classified Information**: BPA does not generate Classified Information. Clearance holders who are responsible for handling this information follow BPA Procedure 433-1-1.

B. **Identifying Controlled Unclassified Information**: For each category below, tools and resources are available on the Information Security homepage. Personnel should consult the Critical Information List and the Information Decision Flowchart during this step.

1. **Official Use Only:**

a) Analyze the information to determine if it has the potential to damage governmental, commercial or private interests, AND

b) Determine if it falls under at least one of the FOIA exemptions 2 – 9. In general, BPA's OUO information falls under FOIA exemptions 4, 5, and 6:

i) BPA uses FOIA Exemption 4 as required by law to protect the trade secrets and confidential commercial or financial information of third parties.

ii) BPA uses FOIA Exemption 5 as permitted by law to protect internal or intra-agency privileged information. Information that qualifies for protection under Exemption 5 must be released if release would not harm the interest protected by a civil discovery privilege, including but not limited to the deliberative process privilege, attorney work-product privilege, and attorney-client privilege.

iii) BPA uses FOIA Exemption 6 as required by law to protect the privacy interests of individuals. Where required, FOIA Exemption 6 is used in conjunction with the Privacy Act.

iv) BPA uses other FOIA exemptions as permitted or required by law.

For more information about these FOIA exemptions, see BPA Policy 236-30 (FOIA).

If the information meets these two criteria, security controls are required. Refer to BPA Procedure 433-1-2 for further instructions.

2. **BES Cyber System Information:** Analyze the information for its potential to be used to gain unauthorized access or pose a security threat to high or medium impact BES Cyber Systems. If the information pertains to either of the topics below, security controls are required:

a) High Impact ratings apply to each BES Cyber System used by or located at BPA's Control Centers, and which perform functions pertaining to reliability, balancing, transmission, or generation authorities or operators, or:

b) Medium Impact ratings apply to BES Cyber Systems not included in High Impact installations, but associated with transmission facilities operating at more than

200kV per line, and which are connected to generation, transmission, or reactive facilities, the failure of which, within fifteen minutes of scheduled operation, could adversely impact the reliable operation of the Bulk Electric System.

If the information meets one of these criteria, security controls are required. Refer to BPA Procedure 433-1-3 for further instructions.

3. **Critical Information:**

   a) Analyze the information to determine if it reveals an operational vulnerability about BPA that an adversary could use to plan an attack, and has been determined to be neither OUO nor BES CSI.

   b) If the information meets this criterion, and has already been determined to be neither OUO nor BES CSI, it is Critical Information. Security controls are required. Refer to BPA Procedure 433-1-4 for further instructions.

C. **Unclassified Information:** If the document does not fall into any of the above categories, it is considered "Unclassified" and security controls are not required.

D. **For Assistance with the Identification Process:** Contact the Information Security Office for assistance with any phase of the of the identification process at informationprotection@bpa.gov.

E. **Reporting Information Security Concerns:** All employees are responsible for reporting loss, misuse, mistreatment of information, and any other concerns to informationprotection@bpa.gov.

9. Performance & Monitoring

A. The Information Security Team conducts an annual assessment of adherence to Information Protection protocols. The team identifies deficiencies, assigns remediation actions, and provides a full findings report to key stakeholders and management. Remediation actions are recorded and tracked on the Information Protection Event Tracking Log.

B. The Office of Security and Continuity of Operations (OSCO) conducts an annual internal self-assessment in order to ensure policy and program effectiveness.

C. The OSCO participates in the Department of Energy self-assessment by providing quarterly reporting.

10. Authorities & References

A. Executive Order 13526, Classified National Security Information, December 29, 2009

B. Executive Order 12958, Classified National Security Information

C. Executive Order 13556, Controlled Unclassified Information

D. Atomic Energy Act, Section 142 and section 144b, as amended, 42 U.S.C. 201

E. Information Security Oversight Office, NARA, Proposed Rule RIN 3095-AB80, Controlled Unclassified Information, 32 CFR Part 2002, April 27, 2015

F. DOE O 475.2B, Identifying Classified Information

G. DOE O 471.6, Information Security, June 20, 2011

H. DOE O 471.3, Chg1, Identifying and Protecting Official Use Only Information, April 9, 2003

I. Freedom of Information Act, (FOIA), 5 U.S.C. § 552 (2002)

J. North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards CIP-002-5.1 thru CIP-011-2

11. Review

This policy will be reviewed annually or within 90 days of the effective date of a new or updated DOE Order affecting the Information Security Program.

12. Revision History

This chart contains a history of the revisions and reviews made to this document.

Version Number	Issue Date	Brief Description of Change or Review
V. 3	02-23-2016	BPA Policy 433-1 supersedes BPAM 1072.
V.2	04-04-2014	Migration of content to new BPA policy format (BPAM 1072: Identification and Protection of BPA's Sensitive Information). BPAM 1072 superseded the policy portion of Chapter 300-2
V. 1	02-23-2013	First version of Information Security's Policy and Procedures published as Security Standards Manual Chapter 300-2: Identification and Protection of Sensitive Information

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

BPA Policy 430-2

Managing Access and Access Revocation for NERC CIP Compliance

Table of Contents

430-2.1 Purpose & Background

To assign responsibilities and identify the actions required for the timely review and revocation of authorized unescorted physical access and authorized electronic access to Bulk Electric Systems (BES) Cyber Assets (BCAs), as BCAs are defined in the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) version 5/6 standards.

430-2.2 Policy Owner

The Deputy Administrator working through BPA's Federal Energy Regulatory Commission (FERC) Compliance Manager and the Chief Security and Continuity Officer owns the policy. The CIP Reliability Standard Owner (CIP RSO) has overall responsibility to monitor, report, deploy, evaluate, and propose revisions to this policy.

430-2.3 Applicability

This policy applies to all personnel with authorized unescorted physical access and authorized electronic access to BPA sites and/or systems; BPA managers and supervisors who monitor the performance of federal employees; and Contracting Officers Technical Representatives (COTRs) who oversee the work assignment of contract workers.

430-2.4 Terms & Definitions

A. **Access Revocation Team (ART)** – The team in Personnel Security responsible for managing and monitoring the revocation process for individuals with unescorted physical and electronic accesses across all BPA facilities and systems and ensuring the processes are compliant with NERC CIP-004-6 R5.

B. **BES Cyber Assets (BCAs)** – A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, mis-operation, or non-operation, adversely impact one or more facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the bulk electric system.

C. **Critical Infrastructure Protection – Reliability Standard Owner (CIP RSO)** – The CIP RSO is an assigned role which has authority and responsibilities for agency-wide NERC CIP implementation. The CIP RSO role is accountable for NERC CIP reliability standard compliance across BPA.

D. **Cyber Assets** – Programmable electronic devices, including the hardware, software, and data in those devices.

E. **Security Privilege Coordinator (SPC)** – A person authorized to administer, monitor, and coordinate access privileges for their area of responsibility.

430-2.5 Policy

A. Ongoing unescorted physical and electronic access privileges are dependent on maintaining authorization to BCAs.

B. Unescorted physical and electronic access to BCAs must be revoked within 24 hours from management's decision that access is no longer required.

C. Quarterly verification of unescorted physical and electronic access to BCAs must be completed for federal employees by their responsible BPA manager and for the contract workforce by the responsible COTR.

D. Unescorted physical and electronic access to BCAs must be revoked if annual NERC CIP training lapses.

430-2.6 Policy Exceptions

There are no exceptions; however, consideration shall be applied for CIP identified exceptional circumstances (e.g. emergency, fire, etc.).

430-2.7 Responsibilities

A. **Supplemental Labor Management Office (SLMO)** is responsible for reporting any changes in status of contractors (CFTE) to the ART prior to the effective date. In the case of an urgent or after-hours termination, notify the ART within four hours.

B. **All Contracting Officers Technical Representatives (COTRs)** of service contractors (non-CFTEs) are responsible for reporting changes in status to the ART. In the case of an urgent or after-hours termination, notify the ART within four hours.

C. **All employees** are responsible for annually completing NERC CIP required training and, when directed, completing all required security actions associated with maintaining authorized unescorted physical and electronic access.

D. **All BPA managers** are responsible for knowing and complying with BPA's access revocation procedures. They are also responsible for reporting personnel actions to Human Capital Management prior to the effective date of the action. In the case of an urgent or after-hours termination, they are responsible for notifying the ART within four hours.

E. **All BPA managers and COTRs** are responsible for complying with this policy and completing the required NERC-CIP Access and Revocation training within seven days of assignment of a role for granting access to BES Cyber Assets.

F. **Human Capital Management Staff in the NH organization** is responsible for updating HRmis with appropriate changes (personnel actions or data changes) reported by responsible managers and COTRs. A HRmis report is generated each business day for use by the ART and Security Privilege Coordinators (SPCs).

G. **Security Privilege Coordinators (SPCs)** are responsible for reviewing transfers, terminations, and other notifications assigned to their group. They are required to initiate revocation of electronic or authorized unescorted physical access to BCAs for federal employees or contractor workforce who no longer requires access.

430-2.8 Standards & Procedures

A. For termination actions:

1) Authorized unescorted physical access and all authorized cyber access, to include Remote Access, to BCAs will be removed within 24 hours of the termination action {CIP-004-6 R5.1, CIP-004-6 R5.3}.

2) Individual electronic user accounts will be deleted from BCAs within 30 calendar days of the effective date of the termination action {CIP-004-6 R5.4}.

3) Passwords will be changed for shared account(s) to BCAs known to the individual within 30 calendar days of the termination action {CIP-004-6 R5.5}.

B. For reassignments and transfers:

1) Authorized unescorted physical access to BCAs that BPA determines are not necessary, and authorized electronic access to individual accounts to BCAs will be removed by the end of the next calendar day following the date that BPA determines that the individual no longer requires retention of that access {CIP-004-6 R5.2}.

2) Passwords will be changed for shared account(s) known to the individual within 30 calendar days following the date that BPA determines that the individual no longer requires retention of that access {CIP-004-6 R5.5}.

430-2.9 Performance & Monitoring

Failure to follow this policy may result in a regulatory violation of NERC CIP-004-6 R1-R5 which could subject BPA to penalties and sanctions. The CIP RSO will track NERC CIP violations and violations of this policy and provide notifications of potential policy violations to the individual's manager. The CIP RSO will determine if escalation is required.

Employees violating this policy are responsible for a) reviewing BPA's access policy and b) retaking the NERC-CIP Access & Revocation training upon each violation of the policy and reporting completion of the training to their manager. Multiple violations will result in the CIP RSO and the responsible manager taking further actions including, but not limited to: a) having the employee's second line manager notify the CIP RSO of completion of training, and/or b) notifying and consulting an Employee Relations Specialist that the employee violated this policy.

430-2.10 Authorities & References

A. BPA Policy 434-1: Cyber Security Program.

B. North American Electric Reliability Corporation – Critical Infrastructure Protection (NERC CIP) version 5/6 standards.

430-2.11 Review

This policy is scheduled for review in 2021.

430-2.12 Revision History

Version	Issue Date	Description of Change
1.0	5/13/2014	Initial publication
2.0	6/30/2016	• Name changed from *BPA Policy 475.1 – Managing Access Authorization to NERC CIP Critical Cyber Assets* to *BPA Policy 430-2 Managing Access Revocation for NERC CIP Compliance*. • Updated to meet NERC CIP-004-6 standard.

BPA Policy 434-1

Cyber Security Program

Table of Contents

1. **Purpose & Background**

This policy sets forth requirements and responsibilities for the Bonneville Power Administration Cyber Security Program (CSP) that protects both Information Technology and grid operations cyber systems. The implementation of this policy shall focus on reduction of risk while remaining consistent with obligations under relevant external regulations (see Authority section below) chiefly Department of Energy orders and directives, and the *Federal Information Security Management Act* and also including provisions to allow implementation of requirements of the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards pursuant to the Energy Policy Act of 2005 (Pub. L. 109-58).

Elements of this policy may provide evidence of compliance with NERC CIP, however this policy is not intended solely to be a NERC CIP policy.

2. **Policy Owner**

The BPA Chief Information Security Officer (CISO) is the owner of this policy.

3. **Applicability**

This policy is applicable to all personnel who use, access, modify, manage, maintain or operate IT or Grid IT equipment, including Transmission-owned or -managed cyber systems.

4. **Terms & Definitions**

Refer to *National Institute of Standards and Technology* (*NIST) Interagency Report (IR) 7298 Revision 1, Glossary of Key Information Security Terms* for additional definition related to cyber security, but not unique to this policy. The NIST IR 7298 Rev 1 includes most of the current terms & definitions used in NIST information security publications and those in the *CNSS Instruction No. 4009, National Information Assurance (IA) Glossary.*

NIST Special Publications and Federal Information Processing Standards contain the definitions for key terms used in the implementation of the IT risk management framework and the *Federal Information Security Management Act.*

Refer to *NERC Glossary of Terms Used in NERC Reliability Standards* for additional definition related to critical infrastructure protection, but not unique to this policy. The NERC Glossary of Terms Used in NERC Reliability Standards includes most of the current terms & definitions used in NERC CIP publications.

1. Administrator. The BPA Administrator. As the CEO of a Power Marketing Administration under the U.S. Department of Energy (DOE), the BPA Administrator is head of a DOE departmental element and a member of senior DOE management.

2. Annual. Occurring within a calendar year, (January 1 through December 31) with no more than 15 months between the events required by external standards.

3. Authorizing Official (AO). An authorizing official (AO) is a federal official with authority to formally assume responsibility for operating a cyber system at an acceptable level of risk to BPA operations (including mission, functions, image, or reputation), BPA assets, or individuals.

4. Chief Information Officer (CIO). An official with overall responsibility for IT procurement, maintenance and operations including the selection and designation of the senior agency information security officer.

5. Chief Information Security Officer (CISO) / BPA Senior Agency Information Security Officer (SAISO). The official who ensures the development and maintenance of information security policies, procedures, and control techniques to address all applicable statutory requirements. Pursuant to FISMA, (§ 3544 (a)(3)(A)), the BPA CISO is the senior agency information security official responsible for carrying out CIO responsibilities under the statute and to act as the authorizing official designated representative.

6. Chief Technical Officer (CTO). The CTO is responsible for BPA Enterprise Architecture for the life-cycle management of information, information resources and related IT investments to maximize investments in information technology and ensure information technology is aligned with strategic goals. The CTO is responsible for the BPA Information Technology Architecture.

7. Cyber System: IT equipment or collections of IT equipment; any technology system (or collections thereof) capable of sending, receiving, or storing electronic data. Synonyms: GridIT, IT, information system, cyber asset, IT system. Examples: computing servers, user workstations, remote terminal units, phasor measurement units, network routers and switches, etc.

8. Information Owner (IO) (aka: Information Steward). Official with operational authority for specified BPA information (including responsibility for establishing controls for its generation, collection, processing, dissemination, storage and disposal); generally a business unit manager or designate.

9. Information System Owner (ISO). An official responsible for the overall procurement, development, integration, modification, or operation and maintenance of one or more cyber systems, including identifying and documenting in the system security plan (SSP): the operation of the information system; unique threats to the information system; and any special protection requirements identified by the information system owner, for each information system for which he or she is responsible.
    a. Establishing, documenting, and maintaining a role-based access model
    b. Approving, granting, and revoking access based on the principle of “least privileged”
    c. Tracking owners and users of shared access accounts
    d. Performing and reporting periodic reviews of access lists
    e. Ensure cyber security testing is performed in a manner that reflects production with minimal impact to operations

f. Developing and maintaining Contingency-Recovery plans, pursuant to this policy

g. Ensuring annual recovery and integrity testing of backup media

h. Ensuring compliance with all other controls set forth in these policies

i. Act as the subject matter expert representatives

j. Reviewing and retaining (for three calendar years) all records of granting, changing, or revocation (to include date) of physical and cyber access

k. Ensuring individuals with access to Critical Cyber Assets (CCAs) comply with all relevant NERC CIP requirements

l. Reviewing and updating all user access quarterly

m. Documenting the results of all user access review activity

10. Information System Security Officer (ISSO) / System Security Manager (SSM). Individual responsible to the ISO, IO and AO for maintaining an adequate operational security for one or more cyber systems. The SSM typically has the detailed technical knowledge and expertise required to manage the security aspects of the cyber system and is generally assigned responsibility for the day-to-day security operations.

11. Information Technology (Title 40 US Code, Section 11101):

    With respect to an executive agency means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use—

    a. of that equipment; or

    b. of that equipment to a significant extent in the performance of a service or the furnishing of a product;

    IT includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources. All IP-addressable equipment or devices are included in this category.

12. Privileged User. Any user who has been granted system administrator or network administrator, e.g. super-user access or root-level access, or has authority to alter the security controls or overall security configuration of a cyber system.

13. System Life Cycle (SLC). Establishes procedures, practices, and guidelines governing Information Technology (IT) strategic planning, asset management, project initiation, concept development, planning, requirements analysis, design, development, integration and test, implementation, operations and maintenance, and disposition of information

systems within BPA. One of the key aspects of the SLC is to ensure an orderly and consistent method of developing and deploying systems.

14. North American Electric Reliability Corporation (NERC): The Federal Energy Regulatory Commission (FERC) appointed Electric Reliability Organization (ERO), responsible for development of the reliability standards for the Bulk Electric System (BES).

15. Critical Infrastructure Protection (CIP): The specific set of reliability standards, developed by NERC, pertaining to the physical and cyber security of BES critical assets. Commonly referred to as "NERC CIP.

16. CIP Exceptional Circumstance: A situation that involves or threatens to involve one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death; a natural disaster; civil unrest; an imminent or existing hardware, software, or equipment failure; a Cyber Security Incident requiring emergency assistance; a response by emergency services; the enactment of a mutual assistance agreement; or an impediment of large scale workforce availability.

5. **Policy**

All BPA Information and Information Systems shall adhere to the provisions specified within FISMA, and further clarified within the following sections.

Management of all BPA-owned or –managed cyber systems must conform to the detailed requirements set forth under the BPA Cyber Security Program Plan, as currently amended.

A. **Assignment of Information System Owner:** All devices that meet the federal definition of IT under title 40 US code shall have an Information System Owner assigned and be included in the inventory of a system security plan as approved by the BPA Office of Cyber Security. Information System Owners will be designated in writing and will be responsible for implementation of all provisions in this policy. An emphasis will be given to implementation of real time automated capability for monitoring vulnerabilities, configuration management, asset management and security event logs.

B. **Cyber Security Risk Management:** A cyber security risk management program must be implemented and maintained to identify, evaluate, reduce, and accept security risk to BPA for all BPA cyber systems. The risk management program will consist of a method to categorize systems based on potential threat and impact to BPA missions, evaluate existing compensating controls, and manage exceptions identified through the program.

C. **Security Assessment and Authorization:** Processes must be in place to ensure adequate security assessment and formal risk determinations or decisions for all BPA information and cyber systems. The AO is formally responsible for accepting risk to the agency and providing Authority To Operate (ATO) for all cyber systems. All systems must be incorporated into the BPA security risk management framework, based on each system's security category.

   Implementation of BPAs' cyber and cyber security systems must meet these objectives:

   1. Periodically assess the security controls in organizational cyber systems to determine if the controls are effective in their application.

2. Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational cyber systems.
3. Authorize the operation of organizational cyber systems and any associated cyber system connections.
4. Monitor cyber system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

D. **Access Control:** Controls for both physical and electronic access must be provided for all personnel, devices and processes before granting any privileges within, or access to BPA cyber systems. Access controls for all BPA cyber systems must be implemented based on the principles of least-privilege and separation of duties.

E. **Awareness and Training:** Security awareness and training must be provided for all personnel with authorized access to cyber systems that support BPA mission functions, pursuant to this policy.

F. **Audit and Accountability**: All cyber systems that support BPA mission functions must incorporate auditing and accountability capabilities commensurate with each cyber system's security category.

G. **Configuration and Change Management:** Configuration and Change Management must be performed for all cyber systems that support BPA mission functions commensurate with each cyber system's security category. The Configuration and Change Management program must be implemented in a manner to track and manage all system changes, in order to reduce the risk of impact to BPA's missions.

H. **Contingency Planning:** Contingency planning must be an integral part of each cyber system's operational profile, commensurate with each system's security category.

I. **Continuous Monitoring:** FISMA directs heads of agencies to place all cyber systems under real time, continuous monitoring. In addition, BPA shall ensure the cyber security program applies a continuous assessment model to all security assessments and cyber system assessments.

J. **Identification and Authentication**: Identification and authentication controls must be commensurate with each cyber system's security category and must be provided for all personnel, devices and processes with authorized access to cyber systems that support BPA mission functions.

K. **Incident Response:** Incident response, i.e., incident handling and management, must be provided for all cyber systems that support BPA mission functions. BPA's specific approach to declaring and responding to CIP Exceptional Circumstances is described in Bonneville Power Administration Manual, Policy 21 and Dispatch Standing Order 136.

L. **Maintenance:** Structured maintenance programs must be in place for all cyber systems that support BPA mission functions, commensurate with each system's status in the BPA Systems Life Cycle (SLC) standard and its security category.

M. **Media Protection:** Media protection must be provided for all cyber systems that support BPA mission functions, commensurate with each cyber system's security category.

N. **Physical and Environmental Protection**: Physical and environmental protection must be provided for all cyber systems that support BPA mission functions, commensurate with each system's security category.

O. **Planning:** BPA must develop, document, periodically update, and implement security plans for their cyber systems that describes the security controls in place or planned for the cyber systems and the rules of behavior for individuals accessing the cyber systems.

P. **Personnel Security**: Personnel security programs must be in place for all personnel who have authorized access to cyber systems that support BPA mission functions, commensurate with each cyber system's security category.

Q. **System and Services Acquisition**: BPA prioritizes system and service acquisition activities to ensure that corrective actions identified in required annual FISMA reporting are incorporated into the capital planning process to deliver maximum security in a cost-effective manner. Funding high-priority security investments supports BPA's objective of maintaining appropriate security controls, both at the enterprise and system levels, commensurate with levels of risk and data sensitivity.

R. **System and Communication Protection**: System and communication protections must be provided for all cyber systems that support BPA mission functions, commensurate with each cyber system's security category. The systems and communication protections must be incorporated into an overall BPA strategy that implements the defense-in-depth security principle.

S. **System and Information Integrity**: System and information integrity programs must be provided for all cyber systems that support BPA mission functions, commensurate with each system's security category.

6. **Policy Exceptions**

Exceptions (to include NERC CIP related Technical Feasibility Exceptions) are defined as any non-conformity of programs, processes, or technologies as they relate to the requirements established within this policy and supporting standards.

All exceptions must be documented within thirty days of identification, and submitted no later than sixty days prior to compliance deadlines for approval by the Chief Information Security Officer (CISO). Documentation of all existing and terminated exceptions shall be maintained and tracked as compliance artifacts.

7. **Responsibilities**

A. **BPA Authorizing Official (AO)**

Responsibilities: grants formal Authority To Operate for information systems according to the BPA security authorization process. Authorizing Officials may, as needs warrant, appoint one or more AO Designated Representatives to act on their behalf. The AO exercises inherent U.S. government authority and must be a federal employee. The AO must have authority to oversee the budget and business

operations of information systems within the BPA. The AO at BPA is a formal delegation available in Section IV of the Cyber Security Program, *Letters of Delegation and Designation*. The BPA AO function is accomplished through the Chief Operating Officer. The AO is the only individual at BPA that can accept risk.

B. **BPA Chief Information Security Officer (CISO) / BPA Senior Agency Information Security Officer (SAISO)**

Responsibilities: develops and maintains the BPA cyber security program and all supporting governance and standards documentation. The CISO is the authorizing official designated representative and the senior agency information security officer with statutory authority and responsibility. The CISO facilitates external and internal information security reviews, and coordinates site visits that support federal and DOE oversight and audits. The CISO provides an independent assessment of all NIST security controls for governance, compliance and oversight, and specific direction, guidance and assistance in order to correct deficiencies. The CISO provides technical testing and control assessment to the FERC governance and compliance office. For information security matters, the CISO serves as the CIO's primary liaison to the agency's AO, information owners, and information system owners. The CISO develops and maintains BPA's information security program to ensure effective implementation and maintenance of required information security policies, procedures, and control techniques. Federal requirements for cyber security are interpreted solely by the CISO. The CISO acts as the AODR.

C. **BPA Authorizing Official Designated Representative**

Responsibilities: The Authorizing Official Designated Representative (AODR) is an organizational official that acts on behalf of an AO to coordinate and conduct the required day-to-day activities associated with the security authorization process. The BPA Authorizing Official Designated Representative is delegated and empowered by the AO to make decisions with regard to the planning and resourcing of the security authorization process, approval of the security plan, approval and monitoring the implementation of plans of action and milestones, and the assessment and/or determination of risk.

D. **Information Owners (IO)**

Responsibilities: Official responsible for determining and declaring the sensitivity of the information created, processed, stored, transferred, or accessed on the information system. Information Owners advise the ISO of any special protection requirements of the information. IOs are responsible to approve and review access to cyber assets and to inform the authorizing official of business or mission risks regarding cyber security vulnerabilities or controls. IOs are responsible to understand how cyber security risks affect the devices and systems that impact their mission.

E. **Information System Owner (ISO)**

Responsibilities: Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of one or more information systems. The ISO is responsible for operating an information system on behalf of one or more Information Owners, who specify the data access requirements and conditions which meet the business requirements supported by the system. The ISO coordinates all aspects of the system from initial concept, through development, to

implementation and system maintenance. The ISO is responsible for the selection, development, maintenance and effective implementation of all applicable security controls for each information system. ISOs are responsible to ensure the IO knows their functional responsibilities and the general cyber security posture of the equipment and systems that support the IO mission functions and sub functions.

F. **Information System Security Officer (ISSO) / System Security Manager (SSM)**

Responsibilities: Responsible for identifying and documenting in the system security plan (SSP): the operation of the information system; unique threats to the information system; and any special protection requirements identified by the ISO, for each information system for which he or she is responsible.

G. **Common Control Provider**

Responsibilities: The common control provider is an individual, group, or organization responsible for the development, implementation, assessment, and monitoring of common controls (i.e., security controls inherited by information systems). Common control providers are responsible for: (i) documenting the organization-identified common controls in a security plan (or equivalent document prescribed by the organization); (ii) ensuring that required assessments of common controls are carried out by qualified assessors with an appropriate level of independence defined by the organization; (iii) documenting assessment findings in a security assessment report; and (iv) producing a plan of action and milestones for all controls having weaknesses or deficiencies. Security plans, security assessment reports, and plans of action and milestones for common controls (or a summary of such information) is made available to the ISO inheriting those controls after the information is reviewed and approved by the senior official or executive with oversight responsibility for those controls.

H. **NERC CIP Senior Manager:**

Responsibilities: BPA shall designate a Senior Manager with overall responsibility and authority for managing the implementation and compliance with NERC CIP standards. Any change to this designation must be documented within thirty calendar days of the effective change. The NERC CIP Senior Manager will ensure that Bulk Electric System (BES) cyber systems, as defined by NERC, have a formally appointed IO and ISO as required by this policy and that all BES assets that meet the federal definition of IT are managed in conformance with this policy and that any conflicts with Department of Energy directives or the BPA Cyber Security Program Plan (CSPP) are resolved or documented as an exception.

8. **Standards & Procedures**

Control families, and the control requirements governing implementations of each control family, are specified in the CSPP and the BPA Information Technology Architecture or elsewhere as indicated.

Cyber Security Program Standards are available on the BPA Office of Cyber Security Intranet Site.

Applicable standards are located or referenced within the Bonneville Information Technology Architecture (BITA) published on the Chief Technical Officer (CTO) SharePoint site.

System Life Cycle (SLC) processes, procedures, document templates, and examples are published on the CTO's SLC SharePoint site.

The Cyber Security Program Plan and associated standards and requirements are located on the BPA Office of Cyber Security Website.

Other procedures and internal requirements to meet specific requirements of federal regulation and NERC CIP standards are located in other documentation as noted in this policy.

9. **Performance & Monitoring**

The GOISSP shall provide quarterly management reporting to the CISO and NERC CIP Senior Manager with regard to agency compliance with this policy.

10. **Authorities & References**

A. E-Government Act of 2002, Public Law 107-347, Title III, Federal Information Security Management Act of 2002 (FISMA), P.L. 107-307, 44 U.S.C. § 3541, et seq. as amended.

B. DOE Order 205.1B, Department of Energy Cyber Security Management Program

C. North American Electric Reliability Corporation – Critical Infrastructure Protection (NERC-CIP) standards

D. FIPS-199 Security Category

E. FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems

F. Government Performance Results Act of 1993 (GPRA), P.L. 103-62, as amended.

11. **Review**

This policy shall be reviewed by the policy owner annually for relevant purpose, content, currency, effectiveness, and metrics.

12. **Revision History**

Version	Issue Date	Description of Change
1.0	12/8/2014	Initial creation by Mike Harris from GOISSM Policy doc.
2.0	1/30/2015	Revisions for Cyber Security Program inclusions
3.0	3/2/2015	Grammatical corrections from RFC, moved a few blocks to appropriate sections, added CIP Exceptional Circumstances – Mike Harris
3.1	5/13/2016	Updates to definitions for consistency across policies, by Mike Harris.

1110.1 PURPOSE

To provide Cyber Security policy on the use of BPA Information Technology Services. This policy applies to all personnel who have authorized access to BPA facilities and sites, including BPA federal and contractor employees and visitors. This policy applies to all BPA IT Equipment as defined in Chapter 1110.

The misuse of BPA IT Equipment and Information Technology Services poses significant risks to mission and business of the BPA.

1110.2 DEFINITIONS

A. Authorized Systems Users are BPA federal and contractor employees who have (1) undergone and passed a background security screening in accordance with current federal requirements; (2) been issued physical access; (3) been issued a logon account to the Bonneville User Domain (BUD) administrative network and/or access to any other BPA computer system or network; and (4) taken the mandatory annual Security and Emergency Management and Cyber Security training and have been validated as completing that training.

B. Blog is short for w***eb Log***. A blog is a Web page that serves as a publicly accessible personal journal for an individual, group, or community, including businesses. Typically updated daily, blogs often reflect the personality of the author.

C. Businesslike is practical and unemotional, purposeful and earnest; exhibiting methodical and systematic characteristics that would be useful in business.

D. BPA Authorized Installers are designated personnel who are authorized to install, update and remove BPA licensed software on workstation (desktop or laptop) computing devices. In addition, BPA Authorized Installers are authorized to install, modify and move BPA IT Equipment.

E. BPA Cyber Security is the official organization responsible for development, issuance, and enforcement of policy relating to BPA IT Equipment. Cyber Security's governance is based on federal laws, regulations, DOE Orders and BPA guidelines. All Cyber Security policies and other materials can be found on the Cyber Security Office web site.

F. BPA federal employees are employees and supervisors employed by the federal government and BPA.

G. BPA's Harassment-Free Workplace Policy is provided by BPA Manual Chapter 400/700A, Appendix A.

H. BPA IT Equipment includes BPA's computer networks and any authorized BPA-owned computing device or component that can be attached or connected to BPA's computer network. BPA IT Equipment includes desktop computers and monitors, laptop and portable computers, software, freeware, personal digital assistants (PDAs), telephones, digital cameras, cell phones, smart phones, facsimile machines, pagers, copiers, photocopiers, printers, scanners, servers, fixed or portable storage devices (flash drives), routers, peripheral devices and multi-purpose machines (combined facsimile, printer and copier).

I. BPA IT Support Staff are designated personnel who are authorized to support and modify certain settings on workstation (desktop or laptop) computing devices. They are reached by contacting the Help Desk.

J. BPA Supervisors are BPA federal employees whose position duties include performance and/or conduct supervision of other BPA federal employees.

K. Broadcast e-mail is the distribution of an e-mail message to a large group (50 or more) of BPA federal and contractor employees, rather than addressing the e-mail message to a limited number of specific, individually-named BPA employees or other recipients.

L. Chain e-mail is the electronic equivalent of the chain letter which is a letter that explicitly directs the recipient to distribute copies of the letter to others.

M. Chat Room is a web site, part of a web site, or part of an online service, that provides a venue for communities of users with a common interest to communicate in real time. Forums and discussion groups, in comparison, allow users to post messages but don't have the capacity for interactive messaging.

N. Configuration Settings are persistent or saved values that describe operational parameters for software, including operating systems and hardware. Configuration settings are standardized at BPA and users are prohibited from changing those settings. For example, password changes are set for every ninety days as a standard configuration setting on the BPA administrative network.

O. Contractor is defined by the Bonneville Purchasing Instructions (BPI) in part 1.8, page 1-5 as a firm or individual that currently has a contract to supply goods or services to BPA.

P. Contractor employee is the employee of a contractor or is an independent contractor who has a contract with BPA to provide personnel to perform specific tasks. The contractor-BPA employee relationship is governed by the BPA contract and managed by the Contracting Officer (CO) and the Contracting Officer's Technical Representative (COTR).

Q. Contracting Officer (CO) is the BPA official delegated to award binding contracts on behalf of BPA to contractors and who is responsible for appointing and Contracting Officer's Technical Representative (COTR) to administer the contract.

R. Contracting Officer's Technical Representative (COTR) is appointed by the Contracting Officer by a delegation letter and administers the contract after it has been awarded. For the purposes of this Chapter, the COTR is the person who performs the day-to-day management of the contract.

S. Controlled Access Point is a restricted communication boundary through which an authorized software connection can be made to a computer system on the other side.

T. Data are the plural of datum and are distinct or discreet pieces of information usually formatted as data types (integer, string, etc.) and can exist electronically in database files, free text files, spreadsheet files. Data typically has no syntactical or grammatical meaning with regard to human use. Computers are capable of using such data.

U. Database is a collection of information stored in a computer in a systematic way, such that a computer program can consult it to answer questions. The software used to manage and query a database is known as a database management system (DBMS).

V. Download is the transfer of electronic files from a source to a destination. **Downloading** is the process of transferring electronic files from a source to a destination.

W. Dual Use IT Equipment is IT Equipment that is used as both Administrative/General Purpose IT Equipment and Operational and Control IT Equipment and that may be authorized for access on the BUD administrative network with Cyber Security's authorization.

X. Electronic mail (e-mail) is the exchange of computer-stored messages and attachments (files) across a network, which includes the Internet, using BPA-provided IT Equipment. The author of an e-mail message creates and sends (including forwarding of and/or replying to a received e-mail message) the e-mail message to one or more recipients by specifying the recipients' e-mail address. An e-mail author can also send a message to several recipients at once using a group e-mail address. Sent and received e-mail messages are stored in electronic mailboxes until retrieved by the e-mail user.

Y. File is an electronic collection of binary digits (bits) and bytes (eight bits) typically characterized by a file name and an extension, although in some operating systems, a file extension is not mandatory. A file may contain text, images, motion pictures, binary data, delimited data, audio samples, Internet pages among others.

Z. Financial Transaction is an exchange or transfer of money from one account to another using BPA IT Equipment.

AA. Freeware may be commercial or non-commercial software that is available to the public at no charge. Often the licensing agreement does not contain terms acceptable to BPA. Freeware is high risk software that is typically not supported by a formal organization nor well tested or built on industry standards. It poses a significant risk to the BPA computing environment and is only permitted with Cyber Security approval. It may not be downloaded or installed without express approval.

BB. Gambling (gaming, betting) is to play at any game of chance for money or other stakes using BPA IT Equipment.

CC. Guidance is information that provides direction or advice as to a decision or course of action.

DD. Improper Use is that which meets the criteria of unsuitable, improper or inappropriate as defined in this Chapter and in additional Cyber Security and Employee Relations policies currently in force.

EE. Incremental Charges are financial charges levied on BPA that can be traced back to the specific usage incidence and the BPA federal and contractor employee responsible for incurring that charge. An example of such a charge would be calls made via cellular phone that are itemized on the monthly bill from the cell phone provider.

FF. Information is data that has been processed to add or create meaning for the person who receives it.

GG. Information Technology (IT) is any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

HH. Internet (or Net or Web or World Wide Web) is a global network connecting millions of computers in which users at any one computer can, if they have system permission, get information from any other computer (and sometimes communicate electronically directly to users at other computers). The interconnections between so many computers and computer users, makes the Internet a highly efficient tool for research and communication. It also poses significant vulnerability to Internet users from malicious software.

II. IT Acquisition Review Board (ITARB) - deleted 01-12-2007. The ITARB ceased functioning during the revision of this document.

JJ. Non-work time is defined as the time before an employee's workday begins, after the workday ends, or during lunch.

KK. Operational and Control IT Equipment is any standalone BPA IT Equipment dedicated full time for control of the BPA electrical system and is not authorized for access on the BUD administrative network without Cyber Security approval.

LL. Password is a confidential/secret string of characters (letters, numbers, and other symbols) used in conjunction with a user ID to authenticate an identity or to verify access authorization.

MM. Personal Financial Transaction is an exchange or transfer of funds (monies) on BPA Equipment to procure personal goods or services or to pay personal invoices or bills.

NN. Personal IT Equipment is any non-BPA IT Equipment.

OO. Personal Use is use of BPA IT Equipment by BPA federal and/or contractor employees for non-BPA business and is defined by BPA Manual Chapter 1110A: Allowance for Limited Personal Use of BPA Information Technology Equipment.

PP. Pornography is pictures and/or writings of sexual activity intended solely to excite lascivious feelings, of a particularly blatant and aberrational kind such as acts involving children, animals, orgies, and all types of sexual intercourse.

QQ. Posting is publishing information, documents, images or audio in an online environment such as a web site, chat room, message board, blog.

RR. Peripheral Devices are computer devices, such as a DVD-ROM drive, flash drive or printer, that is not part of the essential computer, i.e., the memory and microprocessor. Peripheral devices can be external – such as a mouse, keyboard, printer, monitor, external hard drive or scanner – or internal, such as a DVD-ROM drive, DVD-R drive or internal modem. Internal peripheral devices are often referred to as integrated peripherals.

SS. Personally Identifiable Information (PII) is any information about an individual maintained by an agency, including, but not limited to education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual. [Source: Cyber Security Policy BPA-20060809-001]

TT. Presentation Settings refer to the Microsoft Windows Screen Saver Display Properties menu which controls the appearance of the software on the display screen. Display Properties consist of settings for screen resolution and color depth, desktop background image (wallpaper), screen saver settings, configuration, and images, and appearance of windows and buttons.

UU. The Privacy Act of 1974, 5 U.S.C. § 552a (2000) is generally characterized as an omnibus "code of fair information practices" that attempts to regulate the collection, maintenance, use, and dissemination of personal information by federal executive branch agencies.

VV. Remote Access Service (RAS) is the ability to gain authorized access to BPA IT Equipment through a controlled access point from locations outside the BPA work environment. Cisco's Virtual Private Network (VPN) is an example of software used to permit secure authorized access through a controlled access point.

WW. Sensitive Unclassified Information (SUI) includes unclassified information requiring protection mandated by policy or laws, such as Privacy Act Information, proprietary information, Export Control Information (ECI), Unclassified Controlled Nuclear Information (UCNI), and Personally Identifiable Information (PII). [Source: US-DOE: Protection of Sensitive Unclassified Information, Including Personally Identifiable Information, September 6, 2006.]

XX. Shareware is essentially non-commercial software created by independent software developers that is often free but sometimes requires users to pay a license fee. Often the licensing agreement does not contain terms acceptable to BPA. Shareware is also high risk software that is typically not supported by a formal organization and not well tested. It poses a significant risk to the BPA computing environment and is only permitted with Cyber Security approval. It may not be downloaded or installed without express approval.

YY. Standards of Ethical Conduct for Government employees are defined by 5 CFR § 2635.

ZZ. User is any federal and/or contractor employee authorized to use BPA IT equipment.

AAA. User ID (userid, user identification) is one half of the authentication identifier assigned to authorized users that is required with the user's password to access computer systems that require authentication.

BBB. Weapon is any instrument or instrumentality used defensively for fighting, combat, and hunting such as but not limited to a semi-automatic or automatic gun (hand gun, pistol, revolver, rifle, etc.), ammunition, gun parts, sword, knife, missile, spear, bomb, explosive chemicals or parts or incendiaries.

1110.3 POLICY

This policy is promulgated under the authority of Title III – Information Security, Federal Information Security Management Act of 2002, Chapter 35 of Title 44, United States Code, § 3544. Federal agency responsibilities A.3.(C) "developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements."

This policy replaces as of January 03, 2007, the existing BPA Manual Chapters 1110 and 1111 by combining them into one chapter and addressing limited personal use as a distinct subchapter for clarity.

This policy is supplemented by the Program Cyber Security Plan (PCSP) which is posted on the Cyber Security site.

Questions regarding this policy should be sent to the Cyber Security mailbox.

A. PURPOSE AND SCOPE

The purpose of this policy is to provide policy and procedures to federal and contractor employees and supervisors regarding the proper business-related use of BPA Information Technology (IT) Equipment. This policy provides notice to BPA federal and contractor employees and supervisors of the consequences for improper use of BPA IT Equipment. BPA IT Equipment represents a significant investment of BPA resources and its proper use is essential to the efficiency of the service that BPA provides.

This policy applies to all BPA federal and contractor employees. Contractor employee oversight or supervision is the responsibility of the contract company by which the contractor employee is employed. The conduct of the contractor employee in the performance of BPA business is subject to the contents of this Chapter and is managed through the contractual relationship between BPA and the contractor.

B. POLICY STATEMENT FOR BUSINESS-RELATED USE OF BPA IT EQUIPMENT

Except as provided by BPA Manual Chapter 1110A, BPA IT Equipment is to be used **only** by BPA federal and contractor employees who are Authorized System Users and **only** for BPA activities related to and consistent with the performance of BPA's mission and in a manner approved by this policy and consistent with Cyber Security policy or by authorized BPA personnel to determine proper use when this policy does not speak to a particular issue. This policy is intended to apply whether the work of BPA federal and contractor employees is being done within the BPA work environment or working on BPA IT Equipment from a remote location.

C. RESPONSIBILITY FOR PROPER AND APPROPRIATE USE OF BPA IT EQUIPMENT

BPA federal and contractor employees are responsible for knowing and understanding current BPA policy regarding the use of BPA IT Equipment, including the limits to personal use established in Chapter 1110A, and conforming their use to such policy. BPA Supervisors are responsible for ensuring that BPA federal employees, under their supervision are current in their understanding of BPA policy regarding the use of BPA

IT Equipment, monitoring such use, and taking appropriate actions pursuant to BPA policy to correct improper use. Contracting Officers (COs)/Contracting Officer's Technical Representatives (COTRs) are responsible for ensuring that contractor employees through their contractor manager are current in their understanding of BPA policy regarding the use of BPA IT Equipment, monitoring such use, and taking appropriate actions to correct improper use.

D. CONSEQUENCES OF IMPROPER USE OF BPA IT EQUIPMENT

BPA federal and contractor employees having authorized access to BPA IT Equipment have an obligation to understand this policy and to limit their use to the activities it allows. BPA Supervisors and Contracting Officers (COs)/Contracting Officer's Technical Representatives (COTRs) have an obligation to understand this policy and monitor the activities of BPA federal and contractor employees, respectively, sufficiently to ensure that conduct is consistent with this policy. Failure of BPA federal and contractor employees or BPA Supervisors or the CO/COTR to satisfy their obligations may subject the employee to loss of authorized system use and/or in the case of BPA federal employees to possible disciplinary action. Contractor employees may be released in accordance with the contract terms. Improper use that is suspected of violating federal laws will be reported to the appropriate law enforcement agencies.

E. POLICY REGARDING ALL BPA IT EQUIPMENT INVOLVING COMPUTERS

The following guidelines are provided to BPA federal and contractor employees and BPA Supervisors as guidance for the proper use of BPA's IT Equipment. These guidelines do not constitute the totality of rules regarding proper use of BPA's IT Equipment involving computers. For circumstances not covered by these items, see BPA IT Equipment (BPAM 1110.3.B) and the Cyber Security Office web site.

1. Only BPA provided and supported IT Equipment may be connected to BPA IT Equipment. This includes connections of desktop computer systems to BPA computer network and/or connections of any peripheral device to a desktop computer that is connected to the BPA computer network.
2. Only authorized BPA IT Support Staff is permitted to modify the configuration of settings for BPA IT Equipment, including computers. BPA federal and contractor employees may, however, change desktop presentation settings (e.g., wallpaper, screen resolution, speaker volume) as provided for by BPA-approved software. In addition, BPA federal and contractor employees may make modifications under the direction of the Help Desk when troubleshooting problems.
3. Only BPA Authorized Installers are permitted to install, modify, or move BPA IT Equipment. All other persons are not authorized to install, modify or move BPA IT Equipment. Unauthorized movement, modification or installation places the BPA IT Equipment being moved and the BPA computer network in jeopardy. In addition, the location of all BPA IT Equipment must be tracked under BPA's IT Equipment asset management program.
4. No software will be installed on BPA IT Equipment without proper authorization, which must include an approved Cyber Security review. This prohibition includes downloading executable files from the Internet, downloading software purchased by BPA federal and contractor employees for personal use, downloading freeware or shareware, downloading or receiving media for demonstration of Beta versions of software provided by outside vendors or provided by other BPA federal and contractor employees. A list of currently approved software is maintained by BPA's IT Program Management (NJM) organization.

F. GUIDANCE SPECIFIC TO USE OF BPA'S E-MAIL SYSTEM

Authorized system users are encouraged to communicate with others using BPA's e-mail whenever appropriate. However, its use is subject to the following guidelines which are provided to BPA federal and

contractor employees and BPA Supervisors as guidance as to the proper use of BPA's e-mail system. These guidelines do not constitute the totality of rules regarding proper use of BPA's e-mail system. For circumstances not covered by these items, BPA federal and contractor employees and BPA Supervisors should consult the basic policy for use of BPA IT Equipment (BPAM 1110.3.B) and the Cyber Security Office web site.

Cyber Security may disable an e-mail account that is in violation of BPA policy or that poses a threat to the BPA network. Cyber Security may be directed by the Supervisor to disable an e-mail account.

1. The BPA e-mail system and its contents, including attachments, are federal government property. As such, all messages sent with BPA's e-mail system, including those allowed by the Personal Use Allowance (BPAM Chapter 1110A), must be businesslike. Failure to use BPA's e-mail system in accordance with the above can put BPA and BPA federal and contractor employees at risk for legal liabilities, embarrassment, adverse business impacts, and other economic consequences. Upon request to Employee Relations, BPA Supervisors, have the right to review any e-mail messages, including attachments, put on the BPA e-mail system by BPA federal and contractor employees. Cyber Security and Cyber Security directed by law enforcement requests have the right to review any e-mail messages, including attachments, put on the BPA e-mail system by federal and contractor employees. BPA federal and contractor employees who have stored BPA e-mail on personally owned computing devices accept the obligation to make such e-mail available to Cyber Security.
2. BPA e-mail messages could become evidence in legal proceedings. If BPA federal and contractor employees' e-mail messages are requested under the Freedom of Information Act or litigation discovery process, BPA federal and contractor employees will be responsible for reviewing messages in their e-mail storage files and producing any responsive messages. If BPA federal and/or contractor employees store personal files not created for BPA work on BPA IT Equipment, then those files would be subject to disclosure.
3. BPA federal and contractor employees are responsible for the security of their individual BPA e-mail files and any e-mail messages they send using the BPA e-mail system. BPA federal and contractor employees should be aware that message recipients can forward the message to any number of individuals and messages may accidentally be delivered to the wrong recipient. In other words, when a BPA federal and/or contractor employee sends an e-mail message, the sending BPA federal and/or contractor employee has no control where the message may eventually go and who will read it. Care should be taken in both the preparation and sending of e-mail messages to minimize the risk that the messages will be received by unauthorized recipients. Messages sent using the BPA e-mail system and sent outside the BPA work environment will be identified as originating within BPA. Special care should be taken to ensure that such messages will only be received by intended recipients.
4. Because of the difficulty of ensuring complete security (see above), the BPA e-mail system should not be used to communicate sensitive unclassified information (SUI) without the proper safeguards authorized and provided by Cyber Security. When BPA e-mail is the only viable method of completing such communications, BPA federal and contractor employees should use extra care to ensure that the e-mail message is correctly addressed and that it will not be forwarded.
5. If the content of a BPA e-mail message possesses longer-term business value, BPA federal and contractor employees are encouraged to consider other methods of communicating the message, and if BPA e-mail is the appropriate method, to remove the e-mail message from the BPA e-mail system to a more permanent storage system. The minimum period of retention of BPA e-mail is thirty (30) days. All e-mail messages stored in the BPA e-mail system will be automatically purged (deleted) upon the

expiration of that minimum period or the period established by additional policy. Some e-mail messages may constitute Official Records. Specific guidance as to the retention of Office Records is provided in the BPA Records Manual.

6. Only BPA's Standard e-mail services are authorized for installation and/or use on the BPA e-mail system. BPA federal and contractor employees are not authorized to install or access any other e-mail systems (e.g., accessing an e-mail service from the Internet or third-party provider). Use of any other e-mail system or services (e.g., an e-mail service from the Internet or a web-based e-mail system via BPA Internet services) is prohibited.
7. Auto-forwarding of e-mail from the BPA's e-mail system to any other e-mail system is prohibited. Auto-forwarding of a personal e-mail into the BPA e-mail system is also prohibited.
8. Only the BPA Security and Emergency Management Office, BPA Corporate Communications, and the Office of the Chief Information Security Officer (CISO) and such BPA employees and/or organizations designated by the BPA Administrator are permitted to use the BPA e-mail system to broadcast messages. Otherwise, BPA federal and contractor employees are not permitted to use the group addressing capability of the BPA e-mail system to broadcast e-mail messages.
9. Using the BPA e-mail system for fund-raising activities other than by authorized BPA employees is prohibited.
10. Sending any passwords in an e-mail or as an attachment using the BPA e-mail system is prohibited unless the e-mail is encrypted with authorized BPA encryption software. Use of encryption must be approved by Cyber Security.
11. Sending Privacy Act of Personally Identifiable Information (PII) in an e-mail or as an attachment using the BPA e-mail system is prohibited unless the e-mail is encrypted with authorized BPA encryption software. Use of encryption must be approved by Cyber Security.
12. The BPA e-mail system may not be used for any illegal activity as defined by state or federal law, regardless of whether or not the state law applies to BPA. State laws shall include all the states in which BPA operates in which BPA is subject to by contract.
13. The BPA e-mail system may not be used to distribute chain e-mails (i.e., electronic chain letters).

G. GUIDANCE SPECIFIC TO USE OF BPA'S INTRA/INTERNET EQUIPMENT

The following items are provided to BPA federal and contractor employees and BPA Supervisors as guidance to the proper use of BPA's Internet Equipment. This list of guidance items does not constitute the totality of rules regarding proper use of BPA's Internet Equipment. For circumstances not covered by these items, BPA federal and contractor employees and BPA Supervisors should consult the basic policy for use of BPA IT Equipment (BPAM 1110.3.B) and consult with their supervisors and Cyber Security.

1. Because of the continuous and dynamic risk inherent in the necessary connection between BPA Intra- and Internet and the Internet as a whole, BPA is continuously assessing, altering, adjusting and revising its policies and technologies to ensure the security of BPA's Intra- and Internet connections. Cyber Security continuously monitors Internet access and may block access to any Internet site it determines may create an unacceptable risk to BPA.
2. Upon the Supervisor's (federal employees) or the CO/COTR's (contractor employee) or law enforcement's request or as result of an intrusion detection alert or monitoring alert, Cyber Security may at its discretion review an individual's Internet usage.

3. Internet posting of BPA business or security-related information, which includes BPA e-mail addresses, sensitive information or PII, for access either internally or externally is prohibited without authorization. This prohibition applies to static postings and to interactive postings, such as “blog” or “chat room” sites.
4. Because of the mechanics of some kinds of Internet searches, BPA federal and contractor employees who encounter data during authorized, business-related Internet searches that is reasonably likely to violate federal law and/or BPA policy regarding proper use of BPA IT Equipment, should report the occurrence to their BPA Supervisors and/or to the BPA Cyber Security organization and follow instructions from those authorities for preventing recurrence. If BPA federal and contractor employees are notified either electronically or otherwise that their search activities have encountered such data, they should immediately cease and desist from such search and, if necessary, consult with Cyber Security as to how their authorized search activity may be conducted without causing such encounters.
5. BPA federal and contractor employees’ personal (non-business-related) use of BPA Internet Equipment should strictly adhere to the limits set forth in BPAM Chapter 1110A.
6. The following use of BPA’s Internet connection is strictly prohibited and such use may result in disciplinary action: (1) accessing and/or downloading any form of pornography or sexually explicit, or offensive material; (2) accessing on-line gambling or gaming web sites and/or engaging in any on-line gambling or gaming.
7. The following use of BPA’s Internet connection is strictly prohibited unless previously approved and supported by Cyber Security policy: accessing and conducting financial transactions in any form.

H. GUIDANCE SPECIFIC TO USE OF BPA’S REMOTE ACCESS EQUIPMENT

The following items are provided to BPA federal and contractor employees and BPA Supervisors as guidance on to the proper use of BPA’s Remote Access Equipment. This guidance does not constitute the totality of rules regarding proper use of BPA’s Remote Access Equipment. For circumstances not covered by this guidance, BPA federal and contractor employees should consult the basic policy for use of BPA IT Equipment (BPAM 1110.3.B) and consult with their supervisors.

1. The office of the Chief Information Security Officer (CISO) manages the approval of Remote Access Service. Verification, provided by BPA Supervisors, of the business need for Remote Access Services will be required prior to granting authorization.
2. Using BPA IT Equipment via Remote Access Services for personal (non-business-related) use shall strictly adhere to the limits set forth in Chapter 1110A.
3. Authorized connections to BPA IT Equipment using Remote Access Services must be terminated as soon as the need for the use has ceased. Remaining connected to BPA IT Equipment using Remote Access Services for extended periods when there is no need for the connection ties up limited resources. Such connections, when detected will be terminated unless specifically authorized through Cyber Security.
4. Use of non-BPA IT Equipment for remote access is strictly prohibited.

Chapter 1110A: Allowance for Limited Personal Use of BPA Information Technology (IT) Equipment

A. PURPOSE

The purpose of this allowance and exception from BPA's otherwise business-only policy with regards to the use of BPA IT Equipment is to provide guidance to BPA federal and contractor employees and BPA Supervisors regarding the proper personal use of BPA IT Equipment. BPA IT Equipment represents a significant investment of resources by BPA and proper use is essential to the efficiency of the service which BPA was created to provide. BPA federal and contractor employees having access to BPA IT Equipment have an obligation to understand this policy and to limit their use to the activities it allows. BPA Supervisors have an obligation to understand this policy and monitor the activities of their employees sufficiently to ensure that policy limits are adhered to. Failure of BPA federal and contractor employees or BPA Supervisors to satisfy their obligations may subject them to loss of system access, disciplinary actions, and/or immediate contract termination.

This allowance does not modify the requirements of the Standards of Ethical Conduct for employees of the Executive Branch [Title 5 Code of Federal Regulations (CFR), 2635], including the employee's responsibility to protect and conserve Government property, to use it for authorized purposes only, and to use official time in an honest effort to perform official duties [5 CFR 2635.704(a) and (b)]. Nothing in BPAM Chapter 1110A pertains to or restricts use of Government property by an employee to carry out his or her official duties and responsibilities in furtherance of the mission of BPA.

B. POLICY STATEMENT RELATED TO PERSONAL USE OF BPA IT EQUIPMENT

BPA IT Equipment is to be used only for supervisor-authorized activities related to and consistent with the performance of BPA's mission, subject to the limited personal use allowance provided below.

C. LIMITED PERSONAL USE ALLOWANCE

Personal use of designated BPA IT Equipment is allowed within the limits and prohibitions specified in this policy. This allowance does not grant or create an inherent right to use Government resources, and one should not be inferred.

Any personal use, even if ostensibly allowed by this policy, may be further limited or revoked at any time by BPA Supervisors or Cyber Security when circumstances warrant such action.

D. RESPONSIBILITY FOR PROPER AND APPROPRIATE PERSONAL USE OF BPA IT EQUIPMENT

BPA federal and contractor employees are responsible for knowing and understanding current BPA policy regarding the use of BPA IT Equipment, including the limits to the allowance for limited personal use established by BPAM Chapter 1110A, and conforming their use to such policy. BPA Supervisors are responsible for

1. ensuring that BPA federal and contractor employees under their supervision and/or direction remain continuously current in their understanding of BPA policy regarding the use of BPA IT Equipment;
2. monitoring potential misuse as appropriate in conjunction with Cyber Security and Employee Relations; and
3. taking appropriate actions pursuant to BPA policy to correct inappropriate use when inappropriate use is observed or reported.

E. CONSEQUENCES OF IMPROPER PERSONAL USE OF BPA IT EQUIPMENT

Failure of BPA federal and contractor employees or BPA Supervisors to satisfy their responsibility for proper and appropriate personal use of BPA IT Equipment may subject them to loss of system access and/or possible disciplinary actions or immediate contract termination.

F. APPLICATION OF NATIONAL SECURITY LEVELS TO LIMITED PERSONAL USE ALLOWANCE

The limited personal use allowance stated in BPAM Chapter 1110A.C applies to all BPA IT Equipment only when the national security level has been designated as Green. The allowance is further limited when the national security levels are other than Green as follows:

1. When the national security level has been designated as Orange or Red, there shall be no personal use of BPA IT Equipment unless otherwise authorized by Cyber Security.
2. When the national security level has been designated as Yellow, personal use allowance shall be permitted on BPA IT Equipment. However, web site and e-mail blocking may increase as the result of DOE, Homeland Security and other official advisories. Should increased web site and e-mail blocking become necessary, Cyber Security shall use official communication channels to notify the workforce in general provided such advisories are not sensitive or classified.
3. When the national security level has been designated as Green or Blue, the personal use policy shall be permitted on BPA IT Equipment. However, web site and e-mail blocking may increase as the result of DOE, Homeland Security and other official advisories. Should increased web site and e-mail blocking become necessary, Cyber Security shall use official communication channels to notify the workforce in general provided such advisories are not sensitive or classified..
4. In situations, where National Security Levels are not modified but there is a credible threat reported by law enforcement, Homeland Security, or the DOE Inspector General or DOE incident response (CIAC) or other official sources, Cyber Security may revoke limited personal use authorization throughout BPA until the threat has been cleared. Prior and subsequent to revocation or the threat being cleared, Cyber Security shall notify the workforce through official BPA channels.

G. SPECIFIC PROHIBITIONS

In all cases, personal use of BPA IT Equipment on duty time is prohibited. That is, personal use of BPA IT Equipment is only permitted before the workday begins, after the workday ends or during lunch time. The following specific restrictions apply to BPA federal and contractor employees' personal use of BPA IT Equipment:

1. BPA federal and contractor employees are specifically prohibited from using BPA IT Equipment for any personal use that interferes with employees' official duties or reflects badly on the conduct of the federal service (this prohibition includes the use of language that would reflect badly on the federal service in otherwise allowed personal use instances). The prohibition especially prohibits gambling and the viewing or correspondence about and/or trading or procurement of weapons of any kind.
2. BPA federal and contractor employees are specifically prohibited from using BPA IT Equipment for any personal use that has been made unlawful by federal, state or local law (whether or not such state or local law governs the conduct of BPA as a federal agency).
3. BPA federal and contractor employees are specifically prohibited from using BPA IT Equipment to maintain or support a personal private business or to assist family, friends or other persons in such activities.
4. BPA federal and contractor employees are specifically prohibited from using BPA IT Equipment in any personal use that violates the Standards of Ethical Conduct for Government employees.

5. BPA federal and contractor employees are specifically prohibited from personal use of BPA IT Equipment in a way that expressly or impliedly represents that BPA or the federal government has sanctioned or endorsed the specific purpose of the personal use.
6. BPA federal and contractor employees are specifically prohibited from using BPA IT Equipment in any personal use that communicates an express or implied threat or violates BPA's Harassment-Free Workplace Policy.
7. BPA federal and contractor employees are specifically prohibited from using BPA IT Equipment in any personal use that includes communication of material (language and/or pictures) that a reasonable person would find offensive (e.g., hate speech, material that ridicules others on the basis of race, gender, color, religion, disability, national origin, sexual orientation, educational and/or economic level).
8. BPA federal and contractor employees are specifically prohibited from using BPA IT Equipment in any personal use that creates a risk to BPA IT Equipment systems (e.g., when such use creates or increases the possibility of threats to BPA IT Equipment by malicious software [Malware]).
9. BPA federal and contractor employees are specifically prohibited from personal use of Operational and Control IT Equipment such as Instrument Controllers (ICs) under any circumstances.
10. While offsite, BPA federal and contractor employees are not permitted to use BPA IT Equipment to connect "directly" to the Internet using a modem (dial up), wireless or wired connection. All connections must be made to the BPA administrative network using VPN software or authorized software. A violation may result in the revocation of remote access privileges.
11. BPA federal and contractor employees are specifically prohibited from removing BPA IT Equipment from the BPA work environment in order to use such equipment for personal use. However, when there is a BPA business requirement to relocate BPA IT Equipment, such relocation may be done through the BPA established processes.
12. BPA federal and contractor employees are specifically prohibited from making purchases of any product for personal use using BPA IT Internet Equipment.
13. BPA federal and contractor employees are specifically prohibited from personal use of any BPA IT Equipment that is designated for classified use under the National Security Act.
14. BPA federal and contractor employees are specifically prohibited from personal use of BPA IT Equipment that imposes more than minimal additional expense to BPA unless authorized by BPA.
15. BPA federal and contractor employees are specifically prohibited from any personal use of BPA IT Equipment that gives the impression that the user is acting in an official capacity.
16. BPA federal and contractor employees are specifically prohibited from any personal use that requires the downloading (i.e., copying) from any non-BPA IT or BPA IT Equipment of large files (greater than five megabytes) such as documents, attachments, motion or still images, digital audio files, and data into BPA IT Equipment.
17. BPA federal and contractor employees are specifically prohibited from any personal use of a program or Internet site that provides continuous data streams to BPA IT Equipment, even if such streams are not stored as files within BPA IT Equipment (e.g., continuous stock quotes, radio broadcasts, news headlines, weather, etc.).
18. BPA federal and contractor employees are specifically prohibited from creating, downloading, viewing, storing, copying or transmitting sexually explicit or sexually oriented materials using BPA IT Equipment.

19. BPA federal and contractor employees are specifically prohibited from participation in fundraising for any entity or activity other than authorized activity related to the Combined federal Campaign or Associates Functions using BPA IT Equipment.
20. BPA federal and contractor employees are specifically prohibited from participation in any political activity using BPA IT Equipment.
21. BPA federal and contractor employees are specifically prohibited from modification of BPA IT Equipment in any way to facilitate personal or BPA official business use.
22. BPA federal and contractor employees are specifically prohibited from installation of any non-BPA owned software or hardware devices on BPA IT Equipment to facilitate personal use.
23. BPA federal and contractor employees are specifically prohibited from any frequent personal use that may cause congestion, delay, or disruption of service to any BPA IT Equipment, including greeting cards, audio, and streaming video and audio, etc., unless authorized by Cyber Security.
24. BPA federal and contractor employees are specifically prohibited from personal use of BPA IT Equipment that involves unauthorized acquisition, use, reproduction, transmission, or distribution of controlled information (e.g., computer software and data; classified, business sensitive, or other nonpublic data; proprietary data; export controlled software or data; or any information in violation of the Privacy Act, copyright, trademark, or other intellectual property rights beyond fair use).
25. BPA federal and contractor employees are specifically prohibited from personal use of BPA IT Equipment that involves gaining authorized access to internal or external systems or networks.

H. NO PRIVACY EXPECTATION FOR PERSONAL USE

BPA federal and contractor employees should understand that there is no right and should be no expectation of privacy. BPA federal and contractor employees' use of BPA IT Equipment is always subject to supervision and such supervision may include supervisory review, including active monitoring through the use of monitoring tools, of BPA federal and contractor employees' use of BPA IT Equipment and the content of materials stored within BPA IT Equipment. Personal use of BPA IT Equipment by BPA federal and contractor employees implies consent by such employees to such review. BPA federal and contractor employees who wish their personal use activities to be private should not use BPA IT Equipment for personal use.

BPA federal and contractor employees should further understand that the content, whether personal or work related, stored within BPA IT Equipment is the property of BPA and may be disclosed in response to a valid subpoena, warrant, court order (including litigation discovery request), Freedom of Information Act (5 USC 552) request, or other authorized direction (e.g., BPA federal and contractor employees' supervisor, Cyber Security, Inspector General, etc.).

I. GUIDANCE FOR ALLOWED PERSONAL USE

The following examples are provided solely for the purpose of guidance for BPA federal and contractor employees and BPA Supervisors to understand what may be allowed as personal use of BPA IT Equipment. BPA federal and contractor employees and BPA Supervisors should not reply on these examples as specific grants of authority for the uses described. If BPA federal and contractor employees or BPA Supervisors are in doubt about whether a specific personal use is or is not allowed by this policy, they should always seek specific authority from their supervisors and/or Cyber Security.

Examples:

1. Occasionally during work and non-work hours using e-mail or telephone, including voice mail, to keep in touch with family members/or significant others regarding work and/or school schedules (e.g., BPA federal and contractor employees calls or e-mails spouse to inform spouse she will be required to work overtime; BPA federal and contractor employee calls or e-mails dependant's school to confirm time of parent-teacher meeting, etc.). Occasional use is less than ten minutes during duty time unless otherwise authorized by a supervisor. Occasional use in this context are times outside of the non-work time definition.
2. Using e-mail or telephone to check on status of bank, credit union or TSP accounts under the non-work time definition not to exceed two (2) continuous hours in any non-work period.
3. Preparing and storing current resume and related materials on the local hard drive only under the non-work time definition with no time limit.
4. Accessing public library, newspaper and similar publicly available data that does not include downloading (copying) significant amounts of data or printing numerous or large documents on BPA printers under the non-work time definition not to exceed two (2) continuous hours in any non-work period. Any downloading of data must be to the local hard drive and must not occupy more than fifteen (15) percent of the available hard drive storage space.
5. Conducting research regarding personal travel arrangements or consumer matters (e.g., Kelly Blue Book information) on web sites under the non-work time definition not to exceed two (2) continuous hours in any non-work period.
6. Checking current or predicted weather on web sites under the non-work time definition not to exceed two (2) continuous hours in any non-work period.
7. Personal electronic images may be stored on the local hard drive but not on the H: drive or any other network drive, provided such photographs do not occupy more than fifteen (15) percent of the total data storage on the local hard drive, have been scanned for malicious software and are not in violation of any federal or state laws, regulations, policies or DOE Orders.
8. All BPA federal and contractor employees are permitted to use BPA IT Equipment for reasonable personal use via Remote Access Services (Dial-up, Internet, Wireless) on official travel status and in conjunction with a valid telecommuting agreement. The user must access the Internet through an authorized BPA access point using either the VPN software for wired and wireless connections or the authorized software for dial-up. Failure to follow this process may result in the revocation of remote access privileges.

1110.4 RESPONSIBILITIES

A. Federal and contractor Employees are responsible for the knowledge and the understanding of current BPA policy regarding the use of BPA IT equipment, including the limits of personal use, established in Cyber Security Chapter 1110.A, and are to conform to the use of such policy. BPA federal and contractor employees, who have authorized access to BPA IT equipment, have an obligation to understand this policy and to limit their use to the activities as allowed. Failure of BPA ***federal and contractor employees*** or BPA supervisors or CO/COTRs to satisfy their obligations, may subject the employee to loss of authorized system use and/or in the case of BPA federal employees to possible disciplinary action.

B. Supervisors are responsible for ensuring that BPA ***federal employees***, under their supervision are current in their understanding of BPA policy regarding the use of BPA IT equipment, monitoring such use, and taking appropriate actions pursuant to BPA policy to correct improper use. BPA supervisors have an obligation to understand this policy and monitor the activities of BPA federal employees sufficiently to ensure that their conduct is consistent with this policy.

C. Contracting Officers (CO) and Contracting Officer Technical Representatives (COTRs) are responsible for ensuring that ***contractor employees*** working through their contractor manager, are kept current in their understanding of BPA policy regarding the use of BPA IT equipment, monitoring such use, and taking appropriate actions to correct improper (inappropriate) use. BPA Contracting Officers (COs)/Contracting Officer Technical Representatives (COTRs) have an obligation to understand this policy and monitor the activities of ***contractor employees*** sufficiently to ensure that their conduct is consistent with this policy. ***Contractor employees*** who do not comply with the policy may be released in accordance with the contract terms.

D. Contractors are responsible for oversight or supervision of the ***contractor employees*** and ensuring adherence to these policies.

1110.5 PROCEDURES

No information in this section.

1110.6 REFERENCES

A. Pub. L. No. 93-579, Title 5 U.S.C. § 552a, Privacy Act of 1974 (2000)

B. Pub. L. No. 107-347, Title III, 44 U.S.C. § 3544 (a)(3)(C), Information Security, Federal Information Security Management Act of 2002

C. 5 CFR § 2635, Standards of Ethical Conduct for Employees of the Executive Branch

D. 5 CFR § 2635.704(a) and (b), Standards of Ethical Conduct for Employees of the Executive Branch

E. US-DOE: Protection of Sensitive Unclassified Information, Including Personally Identifiable Information, September 6, 2006

F. BPA Manual Chapter 400/700A, Appendix A, BPA's Harassment-Free Workplace Policy

G. BPA Program Cyber Security Plan (PCSP)

H. Cyber Security Policy BPA-20060809-001, Personally Identifiable Information (PII)