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