BPA Policy 433-1

Information Protection

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 requirements for identifying, handling, and controlling CUI. This policy and accompanying procedure for CUI specifies safeguarding requirements 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. Personnel with classified security clearances are authorized by the Department of Energy to handle classified information.

2. Policy Owner

A. The Chief Administrative Officer is the owner of this policy.

B. The Office of Security and Continuity of Operations is responsible for the Information Security program. For questions regarding safeguarding classified information contact the Information Security program area via email at Informationprotection@bpa.gov.

3. Applicability

This policy applies to safeguarding all sensitive information in the possession or control of Bonneville Power Administration.

4. Terms & Definitions

A. **Controlled Unclassified Information (CUI):** CUI is information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, Government-wide policy (LRGWP) requires or permits an agency to handle using safeguarding or dissemination controls. CUI does not include classified information or information a nonexecutive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency. For further explanation which is important to personnel for consistent use of terms please see Appendix A of this policy.

B. **Critical Information List (CIL):** BPA's agency-wide list of critical information subjects and assets, also includes applicable CUI categories and subcategories of CUI under BPA control requiring safeguards. Only CUI categories and subcategories approved by National Archives and Records Administration (NARA), the CUI Executive Agent (EA), and published in the CUI Registry, may be utilized.

C. **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, and BPA IGLM Policy 236-1.

D. **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.

E. **Sensitive Information:** Classified and Controlled Unclassified Information that requires safeguarding controls.

5. Policy

To ensure the continued security of the power grid and comply with Federal and information security standards, BPA shall establish methods to effectively categorize, safeguard, and control sensitive information under its control. Personnel shall protect this information from unauthorized access to safeguard people, operations, and assets. Federal records containing CUI must be managed according to Information Governance Lifecycle Management (IGLM) policies and procedures for records disposition. The workforce shall adhere to the following safeguards and security controls:

A. **Properly Safeguarding Sensitive Information at BPA**: All BPA workforce shall be trained to identify and safeguard sensitive information throughout its lifecycle and destroying the information once it is superseded or passes its retention period. Mishandled, misused, or lost sensitive information must be reported to informationprotection@bpa.gov. Sensitive information may include information BPA generates in regards to BPA operations or information provided by other entities including other Federal departments or business partners.

1. **Identifying Information (Identify):** All information shall be initially assessed to determine if the information created or received by BPA qualifies as CUI. Information identified as having the potential to damage governmental, commercial or private interests, and meets requirements for identification as a subcategory of CUI under the National Archives and Records Administration (NARA) Information Security Oversight Office (ISOO) CUI Registry or NERC CIP Information Security requirements must be safeguarded following BPA Procedure 433-1-2, Identification and Control of Controlled Unclassified Information (CUI Procedure).

2. **Marking Information (Mark):** Personnel shall clearly mark CUI with the appropriate CUI category.

3. **Controlling Information (Control):** Personnel shall comply with information protection requirements throughout the lifecycle of CUI, from creation to destruction, regardless of form.
4. **Destroying Information (Destroy):** Personnel shall destroy sensitive information when no longer needed utilizing authorized destruction methods consistent with BPA Procedure 433-1-2, Identification and Control of CUI.
5. **Reporting Information Mishandling (Report):** Personnel shall report loss, misuse, or mishandling of CUI to informationprotection@bpa.gov within 24 hours of discovery.

B. **BPA Information Security Program (INFOSEC):** BPA Office of Security and Continuity shall ensure that CUI is safeguarded from misuse. To ensure proper handling of CUI, BPA's Office of Security and Continuity shall establish and maintain a program dedicated to safeguarding CUI to include:

1. Coordination with the Chief Information Officer and NERC CIP Senior Manager on matters related to information protection.
2. Adherence to BPA Self-Assessment Program.
3. Coordinating the development and delivery of the BPA Information Protection Training and Awareness Program.

6. Policy Exceptions

There are no exceptions to this policy.

7. Responsibilities

A. **The Chief Administrative Officer (CAO):** Ensures effective safeguards and security policies and programs are in place at BPA.

B. **The Chief Security and Continuity Officer (CSCO):** Ensures implementation and compliance with DOE Order 471.7, Controlled Unclassified Information, DOE Order 471.6, Information Security 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 CUI.
3. Identification and protection of BES Cyber System Information.
4. Adherence to BPA Self-Assessment Program.
5. Development and delivery of the BPA Training and Awareness Program.
6. 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 information and CUI. 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 (CISO):** Is responsible for the following:

1. Develops and maintains the agency Cyber Security Program (CSP) regarding 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 CIP Reliability Standard Owner 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 Operations Security Working Group representatives and BPA Vice Presidents with cyber security issues related to the electronic management and safeguarding of CUI.
6. Ensures training and appropriate oversight of personnel with significant responsibilities for information security and information technology.

E. **The Freedom of Information Act (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/Information Owners**: Official with operational authority for specific BPA information (including responsibility for establishing controls for its generation, collection, processing, dissemination, storage and disposal); generally a business unit manager or designee. Participate in performance and monitoring activities, including the annual assessment of adherence. Ensure all required personnel:

1. Complete DOE CUI training within thirty days of hire, and bi-annually thereafter.
2. Complete additional BPA Information Protection Training as required.
3. Report loss, misuse, mistreatment of information, and any other information security concerns to informationprotection@bpa.gov.

8. Standards & Procedures

Procedural documents accompanying this policy give specific instructions for the handling of each category of CUI 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:** Links to tools and resources are available on the BPA Connections CUI homepage. Personnel should consult the Critical Information List and the Information Decision Flowchart during this step. If the evaluated information meets CUI criteria, security controls are required. Refer to BPA Procedure 433-1-2, Identification and Control of Controlled Unclassified Information for further instructions.

C. **Identifying Unclassified Information:** If the document does not fall into either 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 during any phase of the of the identification process at informationprotection@bpa.gov.

9. Performance & Monitoring

A. The Information Security Team conducts an annual assessment of adherence to information security controls. The team assesses compliance using specific safeguards and security controls across organizations responsible for identifying, controlling and marking CUI. The team shall identify deficiencies, assign remediation actions, and provide 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 Safeguards and Security Periodic Survey to ensure policy and program effectiveness.

C. The OSCO participates in the Department of Energy self-assessment by providing an annual report.

10. Authorities & References

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

B. Executive Order 13556, Controlled Unclassified Information, November 4, 2010;

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

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

E. DOE O 475.2B, Identifying Classified Information, dated October 3, 2014;

F. DOE O 471.6, Information Security, September 12, 2019;

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

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

I. North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards CIP-002-5.1 thru CIP-011-2 August 12, 2019;

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

Version Number	Issue Date	Brief Description of Change or Review
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
V. 2	1/24/2023	Publication of revised Policy

Appendix A: Controlled Unclassified Information

The following explanations are important to personnel for consistent use of terms and their relationship to Federal requirements. These changes are from previous terms used and help support a common understanding, government wide.

A. Controlled Unclassified Information (CUI): CUI categories approved by National Archives and Records Administration (NARA), the CUI Executive Agent (EA), published in the CUI Registry, and authorized for DOE use, are the exclusive designations for identifying CUI within DOE. No other safeguarding and dissemination controls can be implemented for any controlled unclassified information other than those permitted by the applicable LRGWP and as indicated in the CUI Registry. The CUI Registry can be found at https://www.archives.gov.cui. For information to be identified as CUI, it must be designated as either of the two types of CUI – CUI Basic or CUI Specified.

   1. CUI Basic is the subset of CUI for which the authorizing LRGWP does not set out specific safeguarding or dissemination controls. CUI Basic is handled according to the uniform set of controls identified in 32 CFR Part 2002, DOE O 471.7, Controlled Unclassified Information, and the National Archives and Records Administration Information Security Oversight Office CUI Registry. If safeguarding and dissemination controls are not contained in the LRGWP, CUI Basic controls apply.

   2. CUI Specified is the subset of CUI in which the authorizing LRGWP contains specific handling controls that requires or permits agencies to use, and which differ from those controls for CUI Basic. Safeguarding and dissemination controls contained in LRGWP take precedence over the requirements in 32 CFR part 2002. CUI Basic controls apply whenever CUI Specified controls do not cover the involved CUI.

B. **Critical Energy Infrastructure Information (CEII, WECC definition):** Information related to critical electric infrastructure or proposed critical electric infrastructure, generated by or provided to the Commission or other Federal agency other than classified national security information, that is designated as critical electric infrastructure information by the Commission or the Secretary of the Department of Energy pursuant to section 215A (d) of the Federal Power Act. CEII was formerly known within BPA as Critical Cyber Asset Information (CCAI, and continues to be known as Bulk Electric System Cyber System Information (BES CSI)). CEII is specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure (physical or virtual) that:

   1. Relates details about the production, generation, transmission, or distribution of energy;

   2. Could be useful to a person planning an attack on critical infrastructure;

   3. Is exempt from mandatory disclosure under the Freedom of Information Act, 5 U.S.C. 552 (2000); and

4. Does not simply give the general location of the critical infrastructure.
5. BPA identifies CEII as Federal Information Processing Standards (FIPS) High Category rating as applying 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
6. BPA identifies CEII as FIPS Moderate Category rating applying 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 affect the reliable operation of the Bulk Electric System.

C. **Export Controlled Information (ECI):** Information (which may include technology, technical data, assistance or software), the export (including, as applicable, transfer to foreign nationals within the United States) of which is controlled under the "Export Administration Regulations"(maintained by the U.S. Department of Commerce), the "International Traffic in Arms Regulations" (maintained by the U.S. Department of State), "10 CFR Part 810, Assistance to Foreign Atomic Energy Activities" regulations (maintained by the U.S. Department of Energy), or various trade and economic sanctions (maintained by the U.S. Department of Treasury's Office of Foreign Assets Control).

D. **Official Use Only (OUO):** A legacy category of CUI that requires safeguards and has not been updated with a current CUI marking. 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 (FOIA) (exemptions 2-9).

E. **Privacy Information:** Requirements for the marking and safeguarding of personally identifiable information (PII) under CUI are outlined in DOE O206.1, *Department of Energy Privacy Program*, current version. PII must be handled in accordance to the level of sensitivity, with more sensitive categories, i.e., Social Security Numbers, financial records, and medical records, being safeguarded through encryption or password-protection. Privacy information, in either physical or electronic format, which is collected, used, processed, maintained, stored, shared, or transferred within DOE should be marked and safeguarded under the requirements of this Directive and 32 CFR part 2002. CUI Specified markings may be applicable under the Privacy Act of 1974 (Title 5 U.S. C. 522a) or Office of Management and Budget directives.