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 (IT) and grid Operations Technology (OT) 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* (FISMA) 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 Officer (CIO) 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 OT equipment, including Transmission-owned or Transmission-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.

A. **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.

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

C. **Authorizing Official (AO):** An 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.

D. **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.

E. **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.

F. **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.

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

H. **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.

I. **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.

J. **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.

K. **Information Technology (40 USC § 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.

L. **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.

M. **System Life Cycle (SLC):** Establishes procedures, practices, and guidelines governing 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.

N. **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 BES.

O. **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.”

P. **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 ISO assigned and be included in the inventory of an SSP as approved by the BPA Office of Cyber Security. ISOs 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. **Minimum Security Requirements:** The minimum security requirements cover seventeen security-related areas with regard to protecting the confidentiality, integrity, and availability of BPA information and operational technology systems (cyber systems) and the data or information processed, stored, and transmitted by those systems. Specific requirements are located in the Bonneville Power Administration Information Technology Architecture unless otherwise noted. The SSP will show if scoping and tailoring results in controls, or control enhancements that differ from BITA requirements.

   1. **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.

   2. **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.

   3. **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.

   4. **Certification, Accreditation, and Security Assessments:** BPA's office of Cyber Security will:

a. Periodically assess the security controls in cyber systems to determine if the controls are effective in their application;
b. Work with ISOs to develop and track the implementation of plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) by following the process established for review by the BPA Internal Controls Oversight Team (ICOT), authorize the operation of cyber systems and any associated information system connections; and
c. Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.
d. At a minimum external systems (i.e. Software as a Service, cloud, etc.), general support systems, and common control provider security assessment reports will be review by the ICOT.
e. If a cyber system is contained within an authorization boundary for an existing authorization, has the same general security requirements and is under the same management control, it can "inherit" the authorization provided it has been assessed or is under adequate continuous monitoring. This is subject to review by the ICOT.

5. **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.

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

7. **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.

8. **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.

9. **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.

10. **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.

11. **Risk Assessment**: BPA periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information through means described in the Cyber Security Assessment Program.

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

13. **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.

14. **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. These plans are to be documented or referenced in the SSP.

15. **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. Personnel security requirements and implementation details are located in the BPA internal Policy documents related to Personnel Security.

16. **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. System and Services Acquisition requirements and implementation details are located in the BPA internal Policy documents specifically BPA Policy 473-1, Acquisition of IT Assets.

17. **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.

18. **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 CISO. Documentation of all existing and terminated exceptions shall be maintained and tracked as compliance artifacts.

7. **Responsibilities**

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

Grants formal Authority To Operate for information systems according to the BPA security authorization process. AOs 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 Administrative 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)**

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. The CISO acts as the Authorizing Official Designated Representative (AODR).

C. **BPA Authorizing Official Designated Representative (AODR)**

The 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 AODR 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. **Internal Controls Oversight Team (ICOT)**

All systems needing or in the judgement of the CISO might need a formal risk determination from the authorizing official will be presented to the ICOT. Documentation of the ICOT review of Security Assessments will be kept in the meeting minutes. Assessment materials will be made available a week prior to the ICOT meeting (ICOT meets bi-weekly). Cyber will be asked to give a quick 10 minute overview of the assessment prior to ICOT discussion and to be available to answer questions.

The ICOT has the ability to escalate a Security Assessment to the Audit Compliance & Governance Committee (ACGC) if it warrants discussion at that level, as well as review any risk associated with the assessment. John Hairston sits on this committee.

Once the Security Assessment is reviewed, it will then be presented to the AO for signature. The package presented to the AO would include any open POAMs related to the system. Documentation of this review

E. **Information Owners (IO)**

Official responsible for determining and declaring the sensitivity of the information created, processed, stored, transferred, or accessed on the information system. IOs 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.

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

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 IOs, 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.

1. Establishing, documenting, and maintaining a role-based access model
2. Approving, granting, and revoking access based on the principle of “least privileged”
3. Tracking owners and users of shared access accounts
4. Performing and reporting periodic reviews of access lists
5. Ensure cyber security testing is performed in a manner that reflects production with minimal impact to operations
6. Developing and maintaining Contingency-Recovery plans, pursuant to this policy
7. Ensuring annual recovery and integrity testing of backup media
8. Ensuring compliance with all other controls set forth in these policies
9. Act as the subject matter expert representatives
10. Reviewing and retaining (for three calendar years) all records of granting, changing, or revocation (to include date) of physical and cyber access
11. Ensuring individuals with access to Bulk Electric System (BES) Cyber Systems comply with all relevant NERC CIP requirements
12. Reviewing and updating all user access quarterly

13. Documenting the results of all user access review activity

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

Responsible for identifying and documenting in the 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.

H. **Common Control Provider**

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.

I. **NERC CIP Senior Manager**

Designated 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 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 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, the BPA Policy Library, the SSP, 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 CSPP 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 Transmission Technology Security and Compliance Team 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. 44 USC § 101, E-Government Act, 2002

B. 44 USC § 3541, et seq., Federal Information Security Management Act (FISMA), 2002

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

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

E. FIPS-199, Security Category

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

G. Pub. L. 103-62, as amended, Government Performance Results Act (GPRA), 1993

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 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
3.1	5/13/2016	Administrative updates to definitions for consistency across policies
3.2	6/18/2018	Minor updates to formatting, use of acronyms, two name changes: BES instead of CCA, and TTSCT instead of GOISSM
3.3	8/31/2018	Minor updates required by the ICOT and DOE IG
3.4	6/27/2018	Changed AO responsibility from COO to CAO per approved delegation.