

BPA Policy 430-2

Managing Access and Access Revocation for NERC CIP Compliance

Table of Contents

1. Purpose & Background	2
2. Policy Owner	2
3. Applicability	2
4. Terms & Definitions	2
5. Policy.....	3
6. Policy Exceptions	4
7. Responsibilities	4
8. Standards & Procedures	5
9. Performance & Monitoring	5
10. Authorities & References	5
11. Review	6
12. Revision History	6



1. Purpose & Background

The North American Electric Reliability Corporation (NERC) works to assure the reliability and security of the North American electric grid. Towards ensuring reliability, NERC has established a series of standards that all Bulk Electric System (BES) utilities must follow. The NERC Critical Infrastructure Protection (CIP) standards ensure the protection of all facilities and systems that are critical to the infrastructure. BPA follows these standards to ensure that all BES facilities and systems are secure and protected from unauthorized access.

The purpose of this policy is 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 System Cyber Systems (BCS) and their associated Protected Cyber Assets (PCA), Electronic Access Points (EAP), Physical Access Control Systems (PACS), and Electronic Access Control or Monitoring Systems (EACMS), as defined by NERC.

2. Policy Owner

The Chief Administrative Officer, working through BPA's Federal Energy Regulatory Commission (FERC) Compliance Manager and the Chief Security and Continuity Officer, owns the policy.

3. Applicability

This policy applies to all personnel (Federal or Contractor staff, as well as other utility workers) with authorized unescorted physical access and authorized electronic access to BPA CIP sites and/or systems; BPA managers and supervisors who monitor the performance of federal employees; and Contracting Officers Representatives (CORs) who oversee the assignment of contract workers.

4. Terms & Definitions

- A. **Access Revocation Team (ART):** The team in the Personnel Security organization responsible for managing and monitoring the revocation process for individuals with unescorted physical and electronic access across all BPA facilities and systems and ensuring the processes are compliant with NERC CIP-004 R5.
- B. **BES Cyber System (BCS):** One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.
- C. **BES Cyber Asset (BCA):** 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.

Organization NN	Title Managing Access and Access Revocation for NERC CIP Compliance	Unique ID 430-2		
Author Aaron Stelly	Approved by Robin Furrer, CAO	Date 9/11/2025	Version [Version #3	Page 2

- D. **Cyber Assets:** Programmable electronic devices, including the hardware, software, and data in those devices.
- E. **BES Cyber System Information:** Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements.
- F. **Security Privilege Coordinator (SPC):** A person authorized to administer, monitor, and coordinate access privileges for their BCS area of responsibility.

5. Policy

BPA follows the NERC CIP standards to ensure that all NERC CIP facilities and systems are secured and protected. Towards this effort, BPA assigns duties to ensure proper access to these facilities and systems.

A. **NERC CIP-based Physical and Logical Access to BPA Facilities and Systems:** BPA shall maintain proper access to facilities and systems, consistent with the following:

1. Ongoing unescorted physical and electronic access privileges are dependent on maintaining authorization to BCSs.
2. In all separation cases, BPA managers, CORs, and SLMO must notify the ART as soon as possible, and no later than 4 hours in urgent or after-hour cases. Revocation of access must occur within 24 hours of the separation action.
3. Quarterly verification of the continued need for unescorted physical and electronic access to BCSs must be completed for federal employees by their BPA manager or delegate responsible and for the contract workforce by the COR responsible or delegate.
4. Unescorted physical and electronic access to BCSs and BCSI must be revoked if annual NERC CIP training lapses or if a BPA manager or COR fails to respond to the quarterly access verification request by the designated deadline.

B. **BPA Actions to Maintain Proper Access to Facilities and Systems:** BPA shall take the following actions to ensure compliance with NERC CIP requirements:

1. For separation actions (termination, voluntary separation, retirement, death of employee):
 - a) Authorized unescorted physical access and all authorized cyber access, to include Remote Access, to BCSs and BES Cyber System Information (BCSI) will be removed within 24 hours of the separation action (CIP-004 R5.1).

Organization NN		Title Managing Access and Access Revocation for NERC CIP Compliance		Unique ID 430-2	
Author Aaron Stelly		Approved by Robin Furrer, CAO		Date 9/11/2025	
		Version [Version #3		Page 3	

- b) Individual electronic user accounts will be deleted from BCSs within 30 calendar days of the effective date of the separation action (CIP-004 R5.3).
 - c) Passwords will be changed for shared account(s) to BCSs known to the individual within 30 calendar days of the separation action (CIP-004 R5.4).
2. For reassignments and transfers:
- a) Authorized unescorted physical access to BCSs and authorized electronic access to individual accounts to BCSs that BPA determines are not necessary 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 R5.2).
 - b) Passwords will be changed for shared account(s) known to the individual reassigned or transferred that had access to or knowledge of the password within 30 calendar days following the date that BPA determines that the individual no longer requires retention of that access (CIP-004R5.4).

6. Policy Exceptions

There are no exceptions.

7. Responsibilities

- A. **Supplemental Labor Management Office (SLMO):** responsible for reporting any changes in the 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. **Contracting Officers Representatives (CORs):** those who are representatives of service contractors who are considered (non-CFTEs), are responsible for reporting changes in status to the ART. In the event of an urgent or after-hours termination, notify the ART within four hours.
- C. **All employees:** 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:** responsible for knowing and complying with BPA’s access revocation procedures. They are also responsible for reporting personnel actions to BPA Human Resources Service Center 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.

Organization NN		Title Managing Access and Access Revocation for NERC CIP Compliance		Unique ID 430-2	
Author Aaron Stelly		Approved by Robin Furrer, CAO		Date 9/11/2025	
		Version [Version #3		Page 4	

- E. **All BPA managers and CORs:** 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 Systems.
- F. **BPA Human Resources Service Center Staff:** responsible for updating Personnel systems with appropriate changes (personnel actions or data changes) reported by responsible managers and CORs. A HRmis report is generated each business day for use by the ART and Security Privilege Coordinators (SPCs).
- G. **Security Privilege Coordinators (SPCs):** 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 BCSs for federal employees or contractor workforce who no longer require access.
- H. **CIP Reliability Standard Owners (CIP RSOs):** appointed by his/her Tier II executive with responsibility for overseeing the lifecycle of a NERC reliability standard. The RSO is the primary owner of assigned NERC reliability standards. The RSO is guided by the Reliability Standard Implementation Planning Process (RSIPP) and supporting materials located on an internal SharePoint page. (<https://txportal.bud.bpa.gov/orgs/TA/RSIPP/Pages/RSIPP.aspx>). The RSO is responsible for certifying compliance, representing BPA during internal and external audits, and leading the drafting and implementation of self-reports and mitigation plans. Because of these duties, a RSO must be a Federal Employee.
- I. **CIP Senior Manager:** A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC CIP Standards.

8. Standards & Procedures

None

9. Performance & Monitoring

- A. The Security Governance & Oversight group will track NERC CIP violations. The RSO assigned to CIP-004 R5 will monitor violations of this CIP requirement and/or this policy and provide notifications of potential policy violations to the involved individual’s manager.

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 or their successors.

Organization NN	Title Managing Access and Access Revocation for NERC CIP Compliance		Unique ID 430-2	
Author Aaron Stelly	Approved by Robin Furrer, CAO	Date 9/11/2025	Version [Version #3	Page 5

11. Review

This policy is reviewed by the Manager of Security and Continuity and will be reviewed for errors, omissions and any necessary updates every 5 years.

12. Revision History

Version Number	Issue Date	Brief Description of Change or Review
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 standard.
3.0	7/30/2025	Updated for context and clarity.

Organization NN	Title Managing Access and Access Revocation for NERC CIP Compliance	Unique ID 430-2		
Author Aaron Stelly	Approved by Robin Furrer, CAO	Date 9/11/2025	Version [Version #3	Page 6