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.