NERC CIP Standards

Critical Infrastructure Protection for the Bulk Electric System

OT Security Learning Series

Document 130 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

Information

The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards are mandatory cybersecurity requirements for the bulk electric system (BES) in North America. Unlike voluntary frameworks, NERC CIP carries significant financial penalties for non-compliance, making it one of the most consequential OT security regulations in the world.

NERC CIP establishes baseline cybersecurity requirements for entities that own, operate, or use critical assets of the bulk power system. The standards cover everything from asset identification and access control to incident response and recovery planning.

2 Background and Authority

2.1 Regulatory Structure

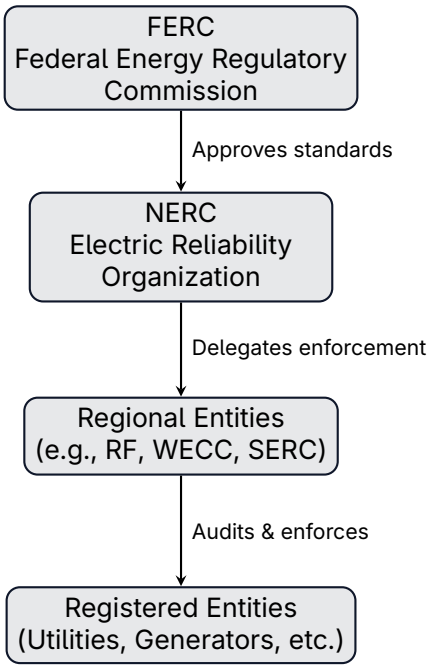

Figure 1: NERC CIP regulatory hierarchy

2.2 History

- **2003** – Northeast blackout highlights grid vulnerabilities
- **2006** – FERC approves first mandatory CIP standards
- **2013** – CIP Version 5 introduces risk-based approach

- **2016** – Supply chain requirements added (CIP-013)
- **Ongoing** – Continuous updates to address emerging threats

3 Applicability

3.1 BES Cyber Systems

NERC CIP applies to Bulk Electric System (BES) Cyber Systems—cyber assets that, if compromised, could affect reliable operation of the grid.

Term	Definition
BES Cyber Asset	Programmable device essential to reliable BES operation
BES Cyber System	One or more BES Cyber Assets logically grouped
Electronic Access Point	Interface controlling routable communication
Physical Security Perimeter	Physical border around BES Cyber Systems
Electronic Security Perimeter	Logical border around BES Cyber Systems

Table 1: Key NERC CIP terminology

3.2 Impact Rating Categories

Systems are categorized by their potential impact on the BES:

Category	Criteria Examples	Requirements
High Impact	Control centers $\geq$3000 MW	Most stringent requirements
Medium Impact	Generation 1500+ MW, transmission substations	Substantial requirements
Low Impact	Remaining BES assets	Baseline requirements

Table 2: BES Cyber System impact categories

Warning

Impact categorization directly determines which CIP requirements apply. Incorrect categorization—whether too low or too high—can result in compliance violations or unnecessary costs.

4 CIP Standards Overview

CIP-002	BES Cyber System Categorization
CIP-003	Security Management Controls
CIP-004	Personnel & Training
CIP-005	Electronic Security Perimeters
CIP-006	Physical Security
CIP-007	System Security Management
CIP-008	Incident Reporting & Response
CIP-009	Recovery Plans
CIP-010	Configuration Management
CIP-011	Information Protection
CIP-012	Communications Between Control Centers
CIP-013	Supply Chain Risk Management
CIP-014	Physical Security (Transmission)

Figure 2: NERC CIP standards family (CIP-001 retired)

5 Key Requirements by Standard

5.1 CIP-002: Categorization

Requires identification and categorization of all BES Cyber Systems:

- Identify BES Cyber Systems at each asset
- Assign High, Medium, or Low impact rating
- Review and update annually
- Senior manager approval required

5.2 CIP-005: Electronic Security

Establishes network security requirements:

- Define Electronic Security Perimeters (ESP)

- Control all inbound/outbound access at Electronic Access Points
- Implement malicious communications detection
- Encrypt remote access sessions

5.3 CIP-004: Personnel & Training

Addresses the human element of security:

- **Security Awareness** – Annual training for all personnel with access
- **Role-Based Training** – Specific training for BES Cyber System access
- **Background Checks** – Personnel Risk Assessments every 7 years
- **Access Management** – Authorize, review quarterly, revoke within 24 hours

5.4 CIP-006: Physical Security

Protects the physical environment around BES Cyber Systems:

- **Physical Security Perimeter** – Defined boundary with access controls
- **Visitor Management** – Continuous escort, logging of visitors
- **Physical Access Monitoring** – Alerts for unauthorized access attempts
- **Access Log Retention** – 90 days minimum

5.5 CIP-007: System Security

Covers technical security controls:

Requirement	Description
Ports and Services	Disable unnecessary ports, document enabled services
Patch Management	Evaluate and apply security patches within 35 days
Malware Prevention	Deploy anti-malware or document mitigations
Security Events	Log and alert on security-relevant events
Access Control	Unique credentials, password complexity, failed login lockout

Table 3: CIP-007 system security requirements

5.6 CIP-008: Incident Response

Mandates incident response capabilities:

- Documented Cyber Security Incident Response Plan
- Defined roles and responsibilities
- Incident reporting to E-ISAC within specified timeframes
- Annual plan testing and updates

5.7 CIP-009: Recovery Plans

Ensures ability to restore BES Cyber Systems:

- **Backup Media** – Protect and test backup media
- **Recovery Plans** – Document procedures for each High/Medium impact system
- **Testing** – Test recovery plans every 15 months
- **Data Preservation** – Retain data for analysis after incidents

5.8 CIP-010: Configuration & Vulnerability Management

Maintains system integrity through change control:

- **Baseline Configuration** – Document OS, firmware, ports, patches
- **Change Management** – Authorize and document all changes
- **Vulnerability Assessment** – Every 15 months minimum
- **Transient Devices** – Control laptops, USB drives in OT environment

5.9 CIP-013: Supply Chain

Addresses third-party risks:

- Develop supply chain risk management plan
- Include security requirements in procurement
- Verify vendor security practices
- Address risks from vendor remote access

Tip

CIP-013 was added after the 2020 SolarWinds incident highlighted supply chain vulnerabilities. It requires entities to assess risks from vendors providing BES Cyber System components.

6 Compliance and Enforcement

6.1 Violation Severity Levels

Level	Severity	Penalty Range (per day)
Lower	Minor documentation gaps	Up to $10,000
Moderate	Moderate risk exposure	$10,000 – $100,000
High	Significant risk	$100,000 – $500,000
Severe	Critical security failure	$500,000 – $1,000,000+

Table 4: NERC CIP violation penalty ranges

Critical

NERC CIP violations can result in penalties up to $1 million per violation per day. In 2019, a single utility was fined $10 million for 127 violations spanning multiple CIP standards.

6.2 Audit Process

- **Self-Certification** – Annual attestation of compliance
- **Spot Checks** – Regional entity verification audits
- **On-Site Audits** – Comprehensive multi-day reviews (every 3 years)
- **Self-Reports** – Entity-initiated violation disclosure

7 Implementation Challenges

7.1 Common Compliance Gaps

- **Asset Inventory** – Incomplete identification of BES Cyber Assets
- **Documentation** – Insufficient evidence of control implementation
- **Change Management** – Unauthorized baseline changes
- **Access Control** – Shared accounts, excessive permissions
- **Patch Management** – Missed 35-day evaluation windows

7.2 OT-Specific Considerations

- Legacy systems may not support required security controls
- Patching must be balanced against operational stability
- Network segmentation can be complex in existing facilities
- Real-time systems have limited logging capabilities

Key Point

Successful CIP compliance requires close collaboration between OT operations, IT security, and compliance teams. Technical controls must be implemented in ways that don't compromise grid reliability.

8 Comparison with Other Standards

Aspect	NERC CIP	IEC 62443	NIS2
Scope	North American BES	Global industrial	EU critical infra
Enforcement	Mandatory, penalties	Voluntary/contractual	Mandatory, penalties
Focus	Prescriptive controls	Risk-based levels	Risk-based measures
Applicability	Electric utilities	All industries	18 sectors

Table 5: Comparison of OT security standards

9 Summary

Key Takeaways

- **Mandatory Standard:** NERC CIP is legally enforceable in North America with significant financial penalties for non-compliance
- **Impact-Based:** Requirements scale based on High, Medium, or Low impact categorization of BES Cyber Systems
- **Comprehensive Coverage:** 13 active standards (CIP-002 through CIP-014, CIP-001 retired) address asset identification, access control, security management, incident response, and supply chain
- **Evidence Required:** Compliance requires documented policies, procedures, and evidence of implementation
- **Supply Chain Focus:** CIP-013 specifically addresses third-party and vendor risks
- **Continuous Process:** Annual self-certifications, regular audits, and ongoing updates require sustained compliance effort

10 Further Reading

Official Sources

- **NERC CIP Standards** – Complete standards library
  https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

- **NERC Compliance Guidance** – Implementation references
  https://www.nerc.com/pa/comp/guidance/Pages/default.aspx

Resources

- **E-ISAC** – Electricity Information Sharing and Analysis Center
  https://www.nerc.com/pa/CI/ESISAC/Pages/default.aspx
- **FERC** – Federal Energy Regulatory Commission
  https://www.ferc.gov/industries-data/electric/industry-activities/cyber-and-grid-security

Books

- Ginter – *SCADA Security* (Abterra Technologies)
- Knapp & Langill – *Industrial Network Security* (Syngress)

Part of the OT Security Learning Series