

NERC CIP v5

NERC CIP is a set of cybersecurity and operational standards to protect bulk electric system infrastructure and ensure grid reliability.



What it is

NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection) is a set of cybersecurity and operational standards that helps organizations in the bulk electric system manage risks to critical infrastructure and protect against cyber threats. These standards are fundamental for ensuring the reliability and security of electric power generation and transmission across North America.

Developed and enforced by NERC, the CIP standards apply to entities that own, operate, or use facilities critical to the operation of the bulk electric system, such as utilities and energy providers. The standards address key areas including cybersecurity controls, physical security, incident response, asset management, and compliance oversight, aligning with broader regulatory frameworks like FERC requirements and industry best practices.

At a glance

PUBLISHER North American Electric Reliability Corporation (NERC)	TYPE Standard	VERSION Current NERC CIP Standards Series
EFFECTIVE April 1, 2016	DOMAIN Cybersecurity	FAMILY Other
REGION United States	INDUSTRY Energy & Utilities	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY Very High		

Source: <https://www.nerc.com/pa/Stand/Pages/USRelStand.aspx>

Why it matters

- **Strengthen critical infrastructure protection** Reduce vulnerabilities in essential electric sector operations through comprehensive cybersecurity and physical security controls.
- **Enhance regulatory compliance** Facilitate adherence to mandatory North American reliability standards, supporting ongoing audit readiness and satisfying FERC requirements.
- **Improve risk management** Enable proactive identification and mitigation of cyber threats targeting generation and transmission assets vital for public safety.
- **Support operational continuity** Promote business resilience by establishing incident response protocols and disaster recovery plans for critical systems.

How SmartSuite supports NERC CIP

BES Cyber System Scope and Categorization

Document BES Cyber Systems, classifications, and scope boundaries with traceability.

CIP Requirement Library

Track CIP requirements with owners, procedures, and implementation evidence.

Access and Change Governance

Manage privileged access, remote access, and change control evidence for OT systems.

Monitoring and Vulnerability Cadence

Schedule logging, patching, vulnerability reviews, and evidence capture consistently.

Incident Response and Recovery Exercises

Run IR and recovery workflows, record results, and track corrective actions.

Audit Readiness Reporting

Provide audit-ready views across requirements, evidence, exceptions, and open gaps.

Common framework mappings

- CIS Controls v8.1
- ISO 27001:2022
- MITRE ATT&CK
- NIS2 (EU 2022/2555)
- NIST CSF 2.0
- NIST 800-53 Rev.5

Official resources

NERC CIP Standards

Defines the requirements for critical infrastructure protection in the bulk electric system.

[nerc.com/pa/Stand/Pages/USRelStand.aspx](https://www.nerc.com/pa/Stand/Pages/USRelStand.aspx)

NERC Glossary of Terms

Provides definitions for terms used in NERC standards, including CIP standards.

[nerc.com/glossary-of-terms](https://www.nerc.com/glossary-of-terms)

NERC Compliance Guidance

Outlines guidance for compliance with NERC standards, supporting regulatory adherence.

[nerc.com/pa/comp/Pages/Default.aspx](https://www.nerc.com/pa/comp/Pages/Default.aspx)

NERC Reliability Standards Development

Describes the process for developing and revising NERC reliability standards.

[nerc.com/standards](https://www.nerc.com/standards)

Frequently asked questions

What is NERC CIP used for?

NERC CIP is used to protect the North American bulk electric system from cybersecurity and physical threats by establishing mandatory security standards for critical infrastructure. It helps utilities and energy providers manage risks to essential assets and ensure the reliability of electric power transmission.

Is NERC CIP mandatory for organizations?

Yes, NERC CIP is a mandatory regulatory framework for entities that own, operate, or use assets critical to the bulk electric system in North America. Compliance is enforced by NERC and subject to oversight by the Federal Energy Regulatory Commission (FERC), with penalties for non-compliance.

Who does NERC CIP apply to?

NERC CIP applies to registered entities such as utilities, transmission operators, and generation companies that are responsible for assets necessary to operate the bulk electric system. The standards are relevant to any organization with control over BES cyber systems, regardless of size.

What core security controls does NERC CIP require?

NERC CIP prescribes controls related to asset identification, electronic and physical access management, incident response, system security management, personnel training, and supply chain risk mitigation. Key artifacts include asset inventories, risk assessments, documented procedures, and access logs.

How are NERC CIP standards implemented in practice?

Organizations implement NERC CIP by conducting asset classification, performing risk assessments, mapping required controls, updating policies, and integrating security safeguards into daily operations. Regular training, documentation, and internal audits help ensure all requirements are met and sustained.

How does NERC CIP relate to other cybersecurity frameworks?

NERC CIP aligns with industry standards like the NIST Cybersecurity Framework and ISO/IEC 27001 by covering similar domains such as risk assessment, incident response, and control management. However, it is uniquely prescriptive and risk-based, specifically tailored to the critical infrastructure of the bulk electric system.

What are the ongoing compliance obligations under NERC CIP?

Organizations must maintain continuous documentation, conduct evidence collection for audits, regularly review risk assessments, and monitor the effectiveness of security controls. Ongoing activities include compliance gap assessments, incident reporting, and participation in NERC CIP audits.

How would SmartSuite support NERC CIP?

SmartSuite supports NERC CIP compliance by providing mapped control libraries, a centralized risk register for BES threats, and policy governance tools for standards management. The platform streamlines evidence collection, automates compliance tracking, enables remediation workflows, and offers comprehensive audit readiness packages and reporting dashboards for effective oversight.

License included / downloadable: Yes NERC CIP standards are publicly available through the North American Electric Reliability Corporation and regulatory agencies.

Full framework page and mappings: smartsuite.com/frameworks/nerc-cip-critical-infrastructure-protection-standards-v5