SmartSuite

Framework / Cybersecurity / Other

NERC CIP Reliability Standards (CIP-002 through CIP-015)

NERC CIP (CIP-002 through CIP-015) are the mandatory cybersecurity and physical security Reliability Standards for the North American bulk electric system, approved by FERC.



What it is

The NERC Critical Infrastructure Protection (CIP) Reliability Standards, CIP-002 through CIP-015, are the mandatory cybersecurity and physical security standards for the North American bulk electric system. The Federal Energy Regulatory Commission (FERC) approves them under section 215 of the Federal Power Act, and the North American Electric Reliability Corporation (NERC), the Electric Reliability Organization, and its Regional Entities enforce them against registered entities. In June 2025 FERC counted about 1,673 U.S. entities subject to mandatory CIP compliance.

At a glance

PUBLISHER
North American Electric Reliability Corporation (NERC); approved by FERC under Federal Power Act section 215

TYPE
Standard

VERSION
CIP-002 through CIP-015 (each standard has its own version; the 2028 virtualization set runs from CIP-002-8 to CIP-013-3)

EFFECTIVE
Set per standard: CIP-003-9 April 1, 2026; CIP-012-2 July 1, 2026; virtualization set July 1, 2028; CIP-014-4 and CIP-015-1 October 1, 2028

DOMAIN
Cybersecurity

FAMILY
Other

REGION
United States (FERC-approved, with U.S. effective dates); NERC covers the North American bulk electric system

INDUSTRY
Energy & Utilities

ADOPTION MODEL
Regulatory Compliance

IMPLEMENTATION COMPLEXITY
High

Source: nerc.com/standards/us-reliability-standards

Why it matters

- **Impact-based scoping** CIP-002-5.1a Attachment 1 sets bright-line criteria for high, medium and low impact, such as 1500 MW generation groups and 300 MW load shedding thresholds.
- **Fixed recurring duties** Examples are security patch evaluation at least every 35 calendar days (CIP-007-6 R2) and incident response plan testing at least every 15 calendar months (CIP-008-6 R2).

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports NERC CIP

BES Cyber System Register

Record each BES Cyber System with its CIP-002 impact rating, Attachment 1 criterion, location, owner and associated EACMS, PACS and PCA, with a change history.

CIP Requirement Library

Load requirements and measures by standard and version with owners, effective dates and linked procedures and evidence, including the version scheduled for each later effective date.

Access and Change Evidence

Keep CIP-004 training and personnel risk assessment dates, 24-hour access removals, CIP-005 remote access records and CIP-010 baseline change reviews against their cadences.

Patching and Monitoring Cadence

Schedule the 35-day patch evaluations, 15-day log reviews and 15-month vulnerability assessments, and attach results to the requirement parts.

Incident Reporting and Recovery Tests

Track determination time for Reportable Cyber Security Incidents, the one-hour notice and next-calendar-day attempt notice, and the CIP-008 and CIP-009 test dates.

Audit Evidence Reporting

Report requirements, evidence, potential noncompliance and open mitigation by standard, entity and registered function.

Common framework mappings

CIS Controls v8.1 | IEC 62443 | ISO 27001:2022 | MITRE ATT&CK | NIS2 (EU 2022/2555) | NIST CSF 2.0 | NIST 800-53 Rev.5

Official resources

NERC U.S. Reliability Standards (CIP-002 to CIP-015)

NERC's list of the mandatory U.S. Reliability Standards in effect, including every CIP standard with its effective date.

nerc.com/standards/us-reliability-standards

NERC Glossary of Terms

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

nerc.com/glossary-of-terms

NERC Compliance program

NERC's compliance monitoring and enforcement program for registered entities, including the CIP standards.

nerc.com/programs/compliance

NERC Reliability Standards Development

Describes the process for developing and revising NERC reliability standards.

nerc.com/standards

Frequently asked questions

Who must comply with the NERC CIP standards?

Registered entities that a standard calls Responsible Entities. CIP-002-5.1a lists balancing authorities, certain distribution providers, generator operators and owners, interchange coordinators or authorities, reliability coordinators, transmission operators and transmission owners, and each standard narrows this by facility and impact rating. In Order No. 918, FERC counted about 1,673 U.S. entities subject to mandatory CIP compliance as of June 2025.

How do high, medium and low impact BES Cyber Systems differ?

CIP-002 requires each Responsible Entity to identify and categorize BES Cyber Systems using the bright-line criteria in Attachment 1. A high impact system includes one used at a Reliability Coordinator control center or at a balancing authority control center for generation of 3000 MW or more in a single Interconnection, and medium impact includes systems tied to generation groups of 1500 MW or more. Later standards set stricter requirements for high and medium impact systems than for low impact systems.

Updated Oct 29, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How quickly must a cyber security incident be reported?

CIP-008-6 R4 requires notice to the E-ISAC and, in the United States, the federal center it names (NCCIC, or its successor) within one hour after determining that a Reportable Cyber Security Incident occurred, and by the end of the next calendar day after determining that an incident was an attempt to compromise an applicable system. The plan must be tested at least once every 15 calendar months.

Which CIP versions apply now, and which are coming?

Each standard has its own date. NERC lists CIP-003-9 as effective April 1, 2026 and CIP-012-2 as effective July 1, 2026. Its October 12 to 18, 2026 update lists the virtualization revisions (CIP-002-8, CIP-003-10, CIP-004-8, CIP-005-8, CIP-006-7.1 through CIP-011-4.1 and CIP-013-3) for July 1, 2028, CIP-014-4 and CIP-015-1 for October 1, 2028, CIP-003-11 for July 1, 2029 and CIP-015-2 for October 1, 2029.

What does CIP-015 require?

CIP-015-1 requires internal network security monitoring inside the Electronic Security Perimeter of high impact BES Cyber Systems and medium impact systems with External Routable Connectivity: monitor network data feeds (R1), retain data on activity judged anomalous until the action is complete (R2) and protect the collected data (R3). FERC approved it in Order No. 907 on June 26, 2025 and directed NERC to extend it to EACMS and PACS outside the perimeter, which is the purpose of CIP-015-2.

License included / downloadable: Yes The CIP Reliability Standards are free PDFs on NERC's website, and the FERC orders that approve them are public in the Federal Register; the platform links to the official text and does not reproduce it.

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