CYBERSECURITY · CIP SERIES · EC-WP-200

NERC CIP 101: Foundations of Cybersecurity

Foundational walkthrough of the NERC Critical Infrastructure Protection framework.

CIP is reliability in the operational technology layer. This reference explains why cybersecurity became a mandatory reliability obligation, how CIP-002 sets the scope for everything that follows, what each CIP standard asks of a program, and how the ERO Enterprise monitors and enforces it.

energycomplianceinc.com **OCTOBER 2026**

Disclaimer & Legal Notice

This publication is the work product of Energy Compliance, Inc. and is provided for general information and educational purposes only. It does not constitute legal advice, regulatory guidance, or formal interpretation of any NERC Reliability Standard, FERC order, or Regional Entity directive.

This publication may not be used or cited as authority in any audit, enforcement, regulatory, or legal proceeding. Compliance with NERC Reliability Standards depends on facts and circumstances unique to each registered entity, and the reader should consult qualified counsel and subject matter experts when making compliance decisions.

NERC, FERC, and the names of Regional Entities are referenced here for descriptive purposes only. Energy Compliance, Inc. is not affiliated with, sponsored by, or endorsed by the North American Electric Reliability Corporation, the Federal Energy Regulatory Commission, or any NERC Regional Entity.

Standard versions, effective dates and requirement text cited in this reference were checked against the primary sources listed in Sources and Authorities as of October 2026. Standards change. Confirm the version in force on the date that matters to you.

Energy Compliance, Inc. assumes no responsibility or liability for errors, omissions, or outcomes resulting from the use of this publication.

Foreword

This professional reference is one of a series Energy Compliance, Inc. publishes for registered entities and the people who run their compliance programs.

I have spent more than thirty years on every side of the bulk electric system. I have operated control centers as a Reliability Coordinator, Transmission Operator, and Power System Operator. I have audited grid facilities and signed off on findings as a senior compliance auditor. I have worked enforcement matters from inside the regulator's process. For the last several years I have advised registered entities directly through the firm I founded.

The entities that do reliability well share a habit. They take the standards seriously without confusing them with reliability itself. A NERC Reliability Standard is a floor, not a ceiling. Compliance is something an auditor evaluates; reliability is something a system either delivers or does not. So these entities prepare for audits by building programs that survive real questions, not binders that look thick.

That is the perspective these references try to share. Each one takes a single topic, whether a standard family, an operational function, a regulatory framework, or an emerging industry problem, and walks through how it actually works.

They are written for the compliance manager who wants to understand the system and not just memorize requirements. For the legal counsel who has to brief a board honestly. For the senior operator who has been told that compliance and reliability are

the same thing and suspects they are not. And for the new compliance hire who was handed a binder and told good luck.

These references are not marketing material dressed up as content. They come from three decades of doing this work and watching it succeed and fail. I wrote them in the voice I use in a control room or in front of a Regional Entity audit team: direct, grounded in evidence, and honest about what the standards do and do not require.

Energy Compliance exists because much of the consulting offered to registered entities today is structured for billable hours rather than for outcomes. Every engagement is overseen by a senior practitioner. We do not bring five people to a meeting that needs one. We automate the work that should be automated and apply senior judgment to the work that requires it. If that is what you want in a compliance partner, the back of this reference has our contact information.

If not, the reference still belongs to you. Take what is useful and apply it well. And remember the only test that ultimately matters: when the system needs to perform, does it?

Rob Smith

Founder and Principal, Energy Compliance, Inc.

Executive Summary

Cybersecurity became part of NERC's reliability mandate because the grid changed. Operations that used to be analog and isolated are now digital and networked. The reliability problem became inseparable from the cybersecurity problem, and the law followed: Section 215 of the Federal Power Act defines a reliability standard to include cybersecurity protection. CIP is not an add-on to reliability. It is reliability in the operational technology layer.

This reference is the starting point for the CIP series. It explains where the Critical Infrastructure Protection standards came from, how CIP-002 decides what is in scope, what the governance, personnel, technical, and incident standards ask of a program, and how CIP compliance is monitored and enforced. It is an orientation, not an implementation guide. The requirement text governs; read it.

- Cybersecurity compliance does not make you cybersecure. In my view, the most expensive mistake in CIP is confusing the audit checkbox with the actual mission.
- CIP-002 is the gate. Everything else in CIP runs through it. Get categorization wrong and the entire program is built on the wrong scope.
- High, Medium, and Low Impact are not degrees of importance. They switch on different sets of requirements, so they produce different control architectures with different audit postures.
- The standards establish the floor. The threat environment sits above the floor. A program built only to the floor operates below the threat baseline.
- Personnel and access are where a large share of CIP risk lives. CIP-004 sits with CIP-010 and CIP-007 as the most frequently reported CIP noncompliance in NERC's 2025 annual report.
- Detection, response, and recovery are not post-incident considerations. CIP-008 and CIP-009 make them pre-incident obligations, with plans that must be tested on a schedule.
- CIP keeps moving. CIP-003-9 took effect April 1, 2026, CIP-012-2 on July 1, 2026, and internal network security monitoring and the virtualization revisions are already on the calendar for 2028.

1 Why Cybersecurity Became a Reliability Imperative

This chapter explains why cybersecurity became a formal, mandatory element of Bulk Electric System (BES) reliability. It covers the operational history and the policy record that led to the Critical Infrastructure Protection (CIP) standards, and why cybersecurity was treated as a reliability issue rather than an IT issue.

1.1 The Grid Went Digital

Over the last few decades the industry replaced electromechanical relays, hardwired panels, and analog telemetry with microprocessor relays, digital communications, Supervisory Control and Data Acquisition (SCADA) systems, and networked control centers. The functions did not change. Protection still clears faults. Operators still need to see the system and move it. What changed is that those functions now run on programmable devices that talk to each other over networks.

The benefits are real. Operators get faster data, better situational awareness, and remote control that used to require a truck roll. The cost is that a device that can be programmed can be reprogrammed, and a network that carries commands can carry the wrong ones. Analog equipment failed in ways engineers understood. Digital equipment can also be made to fail on purpose.

1.2 Built for Function, Not Defense

Control systems were designed to work, and to keep working. Availability, performance, and interoperability drove the design. Security was rarely a design input, partly because many of these systems were assumed to be isolated.

That assumption did not hold. The U.S.-Canada Power System Outage Task Force put it plainly in its April 2004 final report: SCADA systems "were developed to maximize functionality and interoperability, with little attention given to cyber security," and many that were intended to be isolated had become directly or indirectly connected to the Internet for business and operational reasons. The same report recounts the January 2003 "Slammer" worm that took down monitoring computers at the idled Davis-Besse nuclear plant.

Remote access, links into the corporate network, and vendor connections all grew the attack surface. So did the sheer complexity of modern control environments, which makes the side effects of a failure or an attack harder to predict.

1.3 What August 2003 Did and Did Not Show

The August 14, 2003 blackout was not a cyber attack. The Task Force's Security Working Group found no evidence that a malicious cyber attack was a direct or indirect cause of the outage. The event timeline was a chain of non-malicious human and computer failures.

The report still matters to CIP because of what the investigators found along the way. They identified areas of concern in electric sector cybersecurity and issued a dedicated group of recommendations on physical and cyber security, Recommendations 32 through 44. The first was "Implement NERC IT standards." Others called for corporate-level IT security governance, controlling access to operationally sensitive equipment, NERC guidance on employee background checks, intrusion detection, and clear authority for physical and cyber security.

Read that list next to today's CIP family and the lineage is obvious. Governance, access control, personnel screening, monitoring, and incident handling were all on the table before mandatory standards existed.

1.4 Why Availability and Integrity Come First

Enterprise information security usually starts with confidentiality: protect the customer records, the financials, the intellectual property. Reliability starts somewhere else. The question CIP asks is whether the systems that monitor, control, and protect the BES will be available when needed and will do what they are supposed to do.

The statute frames it the same way. Section 215 of the Federal Power Act defines "reliable operation" as operating bulk-power system elements within thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures will not occur "as a result of a sudden disturbance, including a cybersecurity incident." A compromised control system that blinds operators, interrupts communications, or interferes with protection is a reliability event, whether or not any equipment is physically damaged.

Confidentiality is not ignored. CIP-011 protects BES Cyber System Information because that information helps an attacker. But the protection exists to prevent compromise that could lead to misoperation or instability, not to protect data for its own sake.

1.5 Operational Technology Versus Information Technology

Operational technology (OT) monitors or controls physical equipment: energy management systems, SCADA, relays, plant controllers, the networks that carry their traffic. Information technology (IT) runs the business: accounting, human resources, email, websites.

The two share hardware, operating systems, and sometimes networks, which is exactly why the line between them matters. CIP draws its line by function and consequence, not by technology or by which department owns the device. A Windows server can be a BES Cyber Asset. A programmable controller on a test bench may not be. Chapter 3 explains how that line is drawn.

1.6 Executive and Engineering Perspectives

For executives, the shift is that cyber risk is now reliability risk, and reliability risk carries regulatory and corporate accountability. Decisions about system architecture, remote access,

vendors, and staffing all move CIP exposure. Those decisions are made in budget meetings, not just in the server room.

For engineers and operators, the shift is that the systems they configure every day are inside the regulatory perimeter. A firewall rule, a new remote connection, or a firmware update is a reliability decision with a compliance record attached.

Chapter Summary

Growing reliance on digital, networked control systems created cyber risks with direct reliability consequences. The 2003 blackout investigation documented those risks and recommended NERC cyber standards, and the Federal Power Act wrote cybersecurity into the definition of reliable operation. Chapter 2 traces the statutory authority and the evolution of the standards themselves.

> **From the Field**
>
> The standards followed the operational reality.
>
> Once operations went digital and networked, the cyber attack surface became a reliability attack surface. The standards recognize that. Programs that do not operate as if it is true keep finding out the hard way.

2 Statutory Authority and the Evolution of NERC CIP Standards

This chapter covers the federal statute that makes the CIP standards mandatory, the regulatory path from the first CIP version to the current family, and the boundaries the statute sets on CIP's reach.

2.1 Section 215 Names Cybersecurity Directly

The Energy Policy Act of 2005 added Section 215 to the Federal Power Act (16 U.S.C. § 824o). Section 215 is the source of mandatory reliability standards in the United States, and it does not leave cybersecurity to inference. It defines a "reliability standard" as a requirement, approved by FERC, "to provide for reliable operation of the bulk-power system," and states that the term includes requirements for the operation of existing bulk-power system facilities, "including cybersecurity protection."

The statute also defines a "cybersecurity incident" as a malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of the programmable electronic devices and communication networks that operate the bulk-power system. From the first day of mandatory standards, cyber protection was part of the reliability mandate, not a later add-on.

2.2 How a CIP Standard Becomes Mandatory

Section 215 assigns the work to an Electric Reliability Organization (ERO) certified by FERC. FERC certified NERC as the ERO in July 2006. NERC develops standards through its Standard Processes Manual, files them with FERC, and FERC approves them under Section 215(d). FERC can also direct NERC to develop a new standard or modify an existing one to address a specific matter under Section 215(d)(5), and it has used that authority repeatedly in the CIP family.

Once approved, a CIP standard is enforced through the same machinery as every other Reliability Standard: NERC's Compliance Monitoring and Enforcement Program (CMEP) in Appendix 4C to the Rules of Procedure, carried out by NERC and the Regional Entities. Chapter 9 covers that machinery.

2.3 Version 1: The Asset-Based Era

FERC approved the first eight CIP standards, CIP-002-1 through CIP-009-1, in Order No. 706, issued January 18, 2008 (Docket RM06-22-000). The same order directed NERC to develop modifications to address specific concerns.

Version 1 was asset-based. CIP-002-1 required each entity to identify its critical assets and critical cyber assets using a risk-based assessment methodology the entity developed, and the

requirements then applied to those critical cyber assets. The approach left a great deal to each entity's judgment. In Order No. 706 FERC directed NERC to provide additional guidance on developing the methodology, required external review of critical asset lists, and directed removal of the "reasonable business judgment" language from the standards. By Version 4, CIP-002-4 had replaced the entity-built methodology with 17 uniform bright-line criteria for identifying Critical Assets.

2.4 Version 5: The Shift to Impact-Based Categorization

FERC approved the Version 5 CIP standards, CIP-002-5 through CIP-011-1, in Order No. 791, issued November 22, 2013 (Docket RM13-5-000). Version 5 retired the Critical Asset and Critical Cyber Asset approach. In its place, CIP-002 categorizes BES Cyber Systems as High, Medium, or Low Impact against bright-line criteria in Attachment 1, and every BES Cyber System is at least Low Impact.

That change is the foundation of the current framework. NERC described Version 5 as moving away from the Version 4 approach of identifying only Critical Assets, and FERC found that categorizing every BES Cyber System offers more comprehensive protection. The question stopped being "which assets are critical" and became "what could this system do to the BES within 15 minutes if it were unavailable, degraded, or misused, and which bright-line criterion does the associated asset meet." NERC lists July 1, 2016 as the effective date for CIP-006-6, CIP-007-6 and CIP-009-6, all still in force.

2.5 The Family Keeps Moving

Since Version 5, the family has been revised by requirement, not by wholesale version. Individual standards now carry their own version numbers. As of October 2026, NERC lists the following CIP standards as mandatory and subject to enforcement:

Standard	Subject	Effective
CIP-002-5.1a	BES Cyber System Categorization	12/27/2016
CIP-003-9	Security Management Controls	4/1/2026
CIP-004-7	Personnel & Training	1/1/2024
CIP-005-7	Electronic Security Perimeter(s)	10/1/2022
CIP-006-6	Physical Security of BES Cyber Systems	7/1/2016
CIP-007-6	System Security Management	7/1/2016
CIP-008-6	Incident Reporting and Response Planning	1/1/2021
CIP-009-6	Recovery Plans for BES Cyber Systems	7/1/2016
CIP-010-4	Configuration Change Management and Vulnerability Assessments	10/1/2022
CIP-011-3	Information Protection	1/1/2024
CIP-012-2	Communications between Control Centers	7/1/2026

Standard	Subject	Effective
CIP-013-2	Supply Chain Risk Management	10/1/2022
CIP-014-3	Physical Security	6/16/2022

Three developments are already on the calendar:

- **Internal network security monitoring.** FERC approved CIP-015-1 in Order No. 907, issued June 26, 2025 (Docket RM24-7-000). It requires monitoring of network activity inside the Electronic Security Perimeter of high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity. The same order directed NERC to extend that monitoring to EACMS and PACS outside the ESP. NERC lists CIP-015-1 as effective October 1, 2028 and CIP-015-2 as effective October 1, 2029.
- **Virtualization.** NERC Project 2016-02 revised most of the family and the Glossary to address virtualization. NERC lists the resulting versions (CIP-002-7, CIP-003-10, CIP-004-8, CIP-005-8, CIP-006-7.1, CIP-007-7.1, CIP-008-7.1, CIP-009-7.1, CIP-010-5, CIP-011-4.1 and CIP-013-3) and the revised Glossary terms as effective July 1, 2028. CIP-002-8 carries the same date. FERC's March 19, 2026 order in Docket RD25-8-000 approved CIP-002-8 and retires CIP-002-7 immediately before CIP-002-8 takes effect, so CIP-002-8 is the categorization standard that applies from July 1, 2028.
- **Further low impact and physical security changes.** NERC lists CIP-003-11 as effective July 1, 2029 and CIP-014-4 as effective October 1, 2028.

Any program document that cites a CIP version should be checked against the NERC standards page before it goes in front of an auditor.

2.6 Same Statute, Same Enforcement

CIP violations are enforced under the same Section 215(e) authority as frequency, voltage, and protection violations. The ERO may impose a penalty on a user, owner, or operator of the bulk-power system for violating a FERC-approved reliability standard after notice and an opportunity for a hearing, and must file notice and the record with FERC. Under Section 215(e)(2), the penalty cannot take effect earlier than the 31st day after that filing, and it is subject to FERC review.

2.7 Jurisdictional Boundaries

Section 215 limits the reach of every Reliability Standard, CIP included. The ERO has authority to develop and enforce standards "for only the bulk-power system," and the statutory definition of the bulk-power system excludes facilities used in the local distribution of electric energy. In NERC's standards, the BES definition implements that boundary: generally, Transmission Elements operated at 100 kV or higher and Real Power and Reactive Power resources connected at 100 kV or higher, subject to the inclusions and exclusions in the Glossary definition.

CIP therefore does not regulate an entity's enterprise network as such. It regulates the Cyber Assets that meet its definitions. Section 3.5 covers what that leaves out.

2.8 Executive and Engineering Perspectives

For executives, the practical point is that CIP obligations are statutory reliability obligations with the same enforcement path as any operating standard. Board reporting on CIP should sit alongside reporting on operations and planning compliance, not in a separate IT risk register.

For engineers, the practical point is version control. A procedure written to the requirement text of a retired version is a finding waiting to happen, and the next round of versions is already scheduled.

Chapter Summary

Section 215 of the Federal Power Act names cybersecurity protection in its definition of a reliability standard. FERC approved the first CIP standards in Order No. 706 in 2008 and the impact-based Version 5 framework in Order No. 791 in 2013. The family has kept changing since, and three more waves of revisions are already scheduled. Chapter 3 turns to scope: who and what CIP actually covers.

> **From the Field**
>
> Each CIP version reflects the threat the standard was last revised to handle. Reading the version history tells you what the framework has learned about adversary behavior.
>
> The CIP family is revised often because the threat keeps changing. CIP-003 alone is on its ninth version, with two more already approved. A program written for the 2016 text will not pass against the 2026 text.

3 Scope and Applicability of the CIP Framework

This chapter covers how CIP applicability is decided: which registered functions are covered, which Facilities and Cyber Assets fall inside the framework, and what CIP deliberately leaves out. In my view, scope is where CIP programs most often go wrong without anyone noticing, because an error here does not look like an error until an auditor applies the definitions.

3.1 Applicability Starts With Function

CIP applies by registered function, not by company size or ownership. CIP-002-5.1a lists its Responsible Entities as the Balancing Authority, certain Distribution Providers, the Generator Operator, the Generator Owner, the Interchange Coordinator or Interchange Authority, the Reliability Coordinator, the Transmission Operator, and the Transmission Owner.

The Distribution Provider entry is narrow on purpose. A Distribution Provider is in scope only if it owns specific protection or restoration equipment: an underfrequency or undervoltage load shedding system of 300 MW or more under a common control system that is part of a program subject to a NERC or regional standard, a Special Protection System or Remedial Action Scheme subject to a standard, a Protection System that applies to Transmission and is subject to a standard, or a Cranking Path element as described in the standard.

3.2 Facilities Inside the BES Boundary

Registration gets an entity to the door. The Facilities section of each CIP standard decides what is inside. For most entities the applicable Facilities are their Facilities that are part of the BES. CIP-002 Requirement R1 then requires the entity to consider six kinds of assets: Control Centers and backup Control Centers; Transmission stations and substations; generation resources; systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths; Special Protection Systems that support reliable operation of the BES; and, for Distribution Providers, the Protection Systems described in the applicability section.

3.3 The BES Cyber Asset Test

Inside those assets, a Cyber Asset is any programmable electronic device, including its hardware, software, and data. A Cyber Asset becomes a BES Cyber Asset when, if rendered unavailable, degraded, or misused, it would within 15 minutes of its required operation, misoperation, or non-operation adversely impact one or more Facilities, systems, or equipment that would affect the reliable operation of the BES.

Two words in that definition do most of the work. "Misused" means the test is not only about failure; a device that works perfectly in an attacker's hands counts. "Redundancy" appears in the next sentence of the definition, which says redundancy of affected Facilities, systems, and

equipment shall not be considered when determining adverse impact. A backup relay does not take the primary relay out of scope.

3.4 From Assets to Systems

BES Cyber Assets are grouped into BES Cyber Systems, defined as one or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity. The grouping is the entity's choice, and it matters, because requirements apply at the system level and the impact rating attaches to the system.

Around each high and medium impact BES Cyber System sit the associated systems that the requirement tables name in their Applicable Systems columns:

- **Electronic Access Control or Monitoring Systems (EACMS):** Cyber Assets that perform electronic access control or monitoring of the ESP or BES Cyber Systems, including Intermediate Systems.
- **Physical Access Control Systems (PACS):** Cyber Assets that control, alert, or log access to the Physical Security Perimeter, excluding locally mounted hardware such as badge readers.
- **Protected Cyber Assets (PCA):** Cyber Assets connected using a routable protocol within or on an ESP that are not part of the highest impact BES Cyber System in that ESP. A PCA takes the impact rating of the highest rated BES Cyber System in the same ESP.

3.5 What CIP Does Not Cover

CIP does not regulate enterprise-wide cybersecurity. Business systems, corporate email, and general IT are outside the framework unless they meet a CIP definition, for example a corporate system that turns out to perform electronic access control for an ESP and is therefore an EACMS. CIP is not a privacy regime. And the cyber standards address physical security only as it protects BES Cyber Systems; CIP-006 governs Physical Security Perimeters around them.

Physical protection of critical Transmission stations and substations themselves is a separate standard. CIP-014-3 applies to Transmission Owners with stations that meet its criteria and to Transmission Operators, and it addresses physical attack rather than cyber compromise.

3.6 Connectivity Is Not Applicability

Connectivity does not make a device a BES Cyber Asset. The 15-minute impact test does. But connectivity does change which requirements apply once a system is in scope. External Routable Connectivity, the ability to access a BES Cyber System from a Cyber Asset outside its ESP over a bi-directional routable protocol connection, is the trigger for a long list of medium impact requirements. Most of CIP-004's training, personnel risk assessment, access management, and revocation requirements, for example, apply to medium impact BES Cyber Systems "with External Routable Connectivity."

Getting this wrong cuts both ways. Treating every connected device as in scope wastes resources. Missing a routable path that creates External Routable Connectivity leaves requirements unimplemented.

3.7 A Note for Inverter-Based Resource Owners

NERC's IBR Registration Initiative added Category 2 Generator Owners and Generator Operators: owners and operators of inverter-based resources that are not BES Facilities but meet the revised registration criteria. NERC's compliance-date document for those entities lists the CIP standards as "Requires Modification." In other words, the CIP standards are not applicable or enforceable for Category 2 facilities unless and until they are modified, and NERC has not yet decided whether they will be. For an entity that owns both BES and Category 2 facilities, CIP scope today still turns on the BES Facilities and the Control Centers that operate them. Watch the Category 2 compliance-date document; NERC updates it alongside its quarterly IBR work plan filings with FERC.

3.8 Executive and Engineering Perspectives

Executives should understand that scope decisions are capital decisions. Moving a remote access path, consolidating control centers, or adding a fleet operations center can move systems between impact levels and change the cost of the program for years.

Engineers and operators should understand which of the systems they touch are BES Cyber Systems, EACMS, PACS, or PCA, because that label determines the procedures they must follow for every change, account, and connection.

Chapter Summary

CIP applicability is functional. Registered function brings an entity in, the BES boundary decides which Facilities are considered, and the 15-minute BES Cyber Asset test decides which Cyber Assets are in scope. Connectivity then shapes which requirements apply. Chapter 4 covers how CIP-002 assigns the impact ratings that drive everything else.

> **From the Field**
>
> CIP applies based on what the asset does, not what it is called. A control system that meets a Medium Impact criterion is Medium Impact, regardless of how the IT department classifies it.
>
> Scope decisions made at registration become program assumptions for years. A scope set wrong at the start is a finding waiting to happen.
>
> Applicability under CIP is determined by the BES Cyber Asset and BES Cyber System definitions. Anything that meets them is in scope. Reading those definitions closely is the single most important hour in CIP program design.

4 Critical Cyber Assets and Impact Categorization

The chapter title uses the term the industry grew up with. "Critical Cyber Asset" was the Version 1 through Version 3 term, and it retired with Version 5. Today the work is BES Cyber System categorization under CIP-002-5.1a. This chapter walks through that process, the bright-line criteria, and the places categorization most often breaks.

4.1 The CIP-002 Process

CIP-002 has two requirements. Requirement R1 requires a process that considers each of the six asset types listed in Section 3.2 and identifies each high impact BES Cyber System and each medium impact BES Cyber System at each asset, and each asset that contains a low impact BES Cyber System. For low impact, the standard expressly says a discrete list of low impact BES Cyber Systems is not required. The obligation is to know which assets contain them.

Requirement R2 requires the entity to review those identifications, and update them if there are changes, at least once every 15 calendar months, and to have its CIP Senior Manager or delegate approve them on the same interval. Both apply even if the entity has nothing to identify.

4.2 High Impact: Control Centers

High impact is reserved for Control Centers and backup Control Centers under Attachment 1, Section 1:

- Reliability Coordinator Control Centers.
- Balancing Authority Control Centers for generation of 3000 MW or more in a single Interconnection, or for assets that meet criterion 2.3, 2.6, or 2.9.
- Transmission Operator Control Centers for assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.
- Generator Operator Control Centers for assets that meet criterion 2.1, 2.3, 2.6, or 2.9.

4.3 Medium Impact: The Bright Lines

Attachment 1, Section 2 sets the medium impact criteria. Each applies to BES Cyber Systems not already high impact.

Criterion	What it covers
2.1	Generation at a single plant location of 1500 MW or more (aggregate highest rated net Real Power capability of the preceding 12 months) in a single Interconnection; only shared BES Cyber Systems that could affect units totaling 1500 MW within 15 minutes

For criterion 2.5 the weight per line is 700 for lines at 200 to 299 kV and 1300 for lines at 300 to 499 kV. The 1500 MW figure recurs throughout. According to the Guidelines and Technical Basis in CIP-002, the drafting team drew it partly from BAL-002's Contingency Reserve requirements, using the most significant Contingency Reserves Balancing Authorities operate, which must cover the most severe single contingency.

4.4 Low Impact: Everything Else That Qualifies

Section 3 of Attachment 1 makes every BES Cyber System not rated high or medium a low impact BES Cyber System if it is associated with a Control Center, Transmission station or substation, generation resource, restoration facility, Special Protection System, or the Distribution Provider Protection Systems in scope. For many generator owners, especially solar, wind, and storage fleets below the medium impact thresholds, low impact is where the whole program lives. Chapter 5 covers what CIP-003 requires for it.

4.5 Architectures, Not Rankings

Every CIP requirement table has an Applicable Systems column, and the impact rating decides which rows apply. CIP-007 Requirement R2's 35-day patch evaluation cycle applies to high and medium impact BES Cyber Systems and their associated EACMS, PACS, and PCA. Most of CIP-004 applies to high impact systems and medium impact systems with External Routable Connectivity. Low impact BES Cyber Systems are governed by the plan required in CIP-003 Requirement R2 and its Attachment 1, and largely not by CIP-004 through CIP-011.

That is why High, Medium, and Low are better read as three different control architectures than as three points on a scale. Each brings a different set of obligations, evidence, and audit questions.

4.6 Where Categorization Goes Wrong

Categorization errors do not need to be exotic to be serious. A plant's aggregate capability crosses 1500 MW after an uprate and nobody reruns criterion 2.1. A fleet consolidates operations into one center and the center's Generator Operator obligations cross criterion 2.11. A Transmission Planner designates a unit under criterion 2.3 and the notice never reaches the CIP team. Each of those is a scope error that the 15-month review in R2 exists to catch.

The ERO Enterprise has also been explicit about one recurring gap. NERC's 2025 annual report notes that the CIP standards do not include a requirement to identify PACS, PCA, or EACMS, yet failing to identify them leads to missed protections under other requirements. The ERO Enterprise's current practice is to process that failure as a single violation of CIP-010 Requirement R1 and document the other missed requirements within it. NERC's Standards Committee authorized drafting under Project 2021-03 on October 15, 2025 to address identification through CIP-002.

4.7 Executive and Engineering Perspectives

For executives, categorization is the point where system design decisions turn into regulatory cost. An architecture choice that adds External Routable Connectivity, or a control center consolidation that crosses a threshold, should be reviewed for CIP impact before it is approved.

For engineers, categorization tells you which requirements apply to the system in front of you. If you cannot say whether a device is a BES Cyber Asset, an EACMS, a PACS, a PCA, or none of these, find out before you change it.

Chapter Summary

CIP-002 identifies high and medium impact BES Cyber Systems against bright-line criteria and identifies the assets that contain low impact systems, with a review and CIP Senior Manager approval at least every 15 calendar months. The rating decides which requirements apply. Chapter 5 turns to the governance standard, CIP-003.

> **From the Field**
>
> The asset list is the foundation of the entire CIP program. If the asset list is wrong, every downstream control is misapplied.

5 Security Management Controls and Governance

This chapter covers CIP-003-9, Security Management Controls, in effect since April 1, 2026. CIP-003 is the governance standard. It assigns accountability, requires policies that reach every other CIP standard, and carries the entire low impact program.

5.1 The CIP Senior Manager

The NERC Glossary defines the CIP Senior Manager as a single senior management official with overall authority and responsibility for leading and managing implementation of, and continuing adherence to, the requirements in CIP-002 through CIP-011. CIP-003 Requirement R3 requires the entity to identify that person by name and document any change within 30 calendar days.

One name, not a committee. The standard puts accountability on an individual with the authority to fund and direct the program. If the named person does not have that authority in practice, the governance structure will show it at audit.

5.2 Delegation

Requirement R4 allows the CIP Senior Manager to delegate authority for specific actions where the CIP standards permit it. The delegation process must be documented, and each delegation must record the delegate's name or title, the specific actions delegated, and the date, be approved by the CIP Senior Manager, and be updated within 30 days of any change. A change in the CIP Senior Manager does not by itself require delegations to be reissued.

5.3 Policies Reviewed Every 15 Months

Requirement R1 requires the entity to review, and obtain CIP Senior Manager approval for, its documented cyber security policies at least once every 15 calendar months. For high and medium impact BES Cyber Systems, the policies must collectively address personnel and training, Electronic Security Perimeters including Interactive Remote Access, physical security, system security management, incident reporting and response planning, recovery plans, configuration change management and vulnerability assessments, information protection, and declaring and responding to CIP Exceptional Circumstances.

For assets containing low impact BES Cyber Systems, the policies must address cyber security awareness, physical security controls, electronic access controls, Cyber Security Incident response, Transient Cyber Asset and Removable Media malicious code risk mitigation, vendor electronic remote access security controls, and CIP Exceptional Circumstances.

Policies are not outcomes. A policy is worth what it drives: procedures people follow and evidence those procedures produce. A policy no one can connect to a procedure is a document, not governance.

5.4 The Low Impact Plan

Requirement R2 requires an entity with at least one asset containing low impact BES Cyber Systems to implement one or more documented cyber security plans that include the six sections of Attachment 1. The standard notes that an inventory of low impact BES Cyber Systems is not required, and lists of authorized users are not required.

Section	What the plan must do
1. Cyber security awareness	Reinforce cyber security practices at least once every 15 calendar months
2. Physical security controls	Control physical access, based on need, to the asset or the locations of the low impact systems, and to the Cyber Assets providing electronic access controls
3. Electronic access controls	Permit only necessary inbound and outbound routable communications crossing the asset boundary (excluding time-sensitive protection or control communications between IEDs), and authenticate Dial-up Connectivity
4. Incident response	Maintain response plans covering identification, classification, response, E-ISAC notification of Reportable Cyber Security Incidents, roles, and handling; test at least once every 36 calendar months; update within 180 days of a test or actual incident
5. Transient Cyber Assets and Removable Media	Mitigate the risk of introducing malicious code through laptops and media, whether the entity or a third party manages them
6. Vendor electronic remote access	Determine, disable, and detect known or suspected malicious communications for vendor electronic remote access

Section 6 is the CIP-003-9 addition. It applies to assets containing low impact BES Cyber Systems that allow vendor electronic remote access, and it requires methods for determining vendor remote access, disabling it, and detecting known or suspected inbound and outbound malicious communications on it. In my view, for generator fleets that rely on vendor remote support, this is the most consequential CIP change of 2026.

5.5 CIP Exceptional Circumstances

Several requirements excuse performance "except under CIP Exceptional Circumstances." The Glossary defines the term as a situation that involves or threatens a risk of injury or death, a natural disaster, civil unrest, an imminent or existing hardware, software, or equipment failure, a Cyber Security Incident requiring emergency assistance, a response by emergency services, the enactment of a mutual assistance agreement, or an impediment of large-scale workforce availability, or similar conditions that impact safety or BES reliability. CIP-003 requires a policy for declaring and responding to them. The exception is only as defensible as the record of when and why it was declared.

5.6 Governance as Evidence

NERC's 2025 annual report states that enforcement cause codes point to lack of, or deficient, policies and procedures as the leading root cause of noncompliance with CIP-010, CIP-007, and CIP-004. Those are operational standards, and their leading root cause is a governance failure. That is the strongest argument there is for treating CIP-003 as the backbone of the program rather than the paperwork at the front of the binder.

5.7 Executive and Engineering Perspectives

For executives, CIP-003 is where accountability is named. Whoever is the CIP Senior Manager should have the authority, the budget line, and the reporting that the title implies.

For engineers and operators, CIP-003 tells you who decides. When a change, an access request, or an exception comes up, the delegation record says who can approve it. If nobody can find that record, nobody has the authority.

Chapter Summary

CIP-003-9 names a single accountable CIP Senior Manager, governs delegations, requires policies reviewed and approved at least every 15 calendar months, and requires a documented plan for low impact BES Cyber Systems that now includes vendor electronic remote access controls. Chapter 6 covers the people side of CIP.

> **From the Field**
>
> Governance is the part of CIP that does not show up on a network diagram. It is also the part the auditor reads first.
>
> A CIP program whose CIP Senior Manager has no real authority over it is a program waiting for that accountability to be assigned at the next finding.

6 Personnel Risk and Access Considerations

This chapter covers CIP-004-7, Personnel & Training, in effect since January 1, 2024. People operate, maintain, configure, and support BES Cyber Systems. Every one of those interactions is a path to misuse, whether by mistake or by intent. CIP-004 manages that path.

6.1 Who CIP-004 Covers

CIP-004 is not an HR standard for the whole workforce. Its requirements attach to people with authorized electronic access or authorized unescorted physical access to applicable systems. Security awareness under Requirement R1 applies to high and medium impact BES Cyber Systems. Training, personnel risk assessment, access management, and revocation apply to high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity, generally including their associated EACMS and PACS.

Low impact access is governed differently, through the physical and electronic access controls in the CIP-003 low impact plan.

6.2 Security Awareness Every Quarter

Requirement R1 Part 1.1 requires security awareness that, at least once each calendar quarter, reinforces cyber security practices for personnel who have authorized electronic or authorized unescorted physical access. The content is flexible. The quarterly cadence is not.

6.3 Role-Based Training

Requirement R2 requires a cyber security training program appropriate to individual roles. Part 2.1 lists the content: cyber security policies, physical and electronic access controls, the visitor control program, handling of BES Cyber System Information, identifying Cyber Security Incidents and making initial notifications, recovery plans, response to incidents, and the risks of interconnectivity with other Cyber Assets, including Transient Cyber Assets and Removable Media. Part 2.2 requires the training to be completed before access is granted, except during CIP Exceptional Circumstances. Part 2.3 requires it at least once every 15 calendar months.

6.4 Personnel Risk Assessment

Requirement R3 requires a personnel risk assessment program. It includes a process to confirm identity and a seven-year criminal history records check covering current residence and every other location where the person lived for six consecutive months or more during the prior seven years. Part 3.5 requires a process to ensure that individuals with access have a personnel risk assessment completed within the last seven years. Contractors and vendors are covered too.

Part 3.4 requires criteria or a process for verifying that personnel risk assessments performed for contractors or service vendors meet Parts 3.1 through 3.3.

6.5 Access Management

Requirement R4 requires a process to authorize electronic access and unescorted physical access into a Physical Security Perimeter, based on need. Requirement R6 separately governs authorizing, verifying, and revoking provisioned access to BES Cyber System Information. Part 4.2 requires verification at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records. Part 4.3 requires verification at least once every 15 calendar months that all user accounts, account groups or role categories, and their privileges are correct and necessary.

The quarterly verification is a reconciliation: the list of people authorized against the list of people provisioned. It is designed to find access that should not exist. A review that never finds anything is worth a second look.

6.6 Revocation

Requirement R5 sets the clocks that produce findings when they slip:

- **Termination:** initiate removal of the individual's unescorted physical access and Interactive Remote Access upon a termination action and complete those removals within 24 hours of the termination action (Part 5.1).
- **Reassignment or transfer:** revoke electronic access to individual accounts and unescorted physical access the entity determines is no longer necessary by the end of the next calendar day after that determination (Part 5.2).
- **Non-shared accounts on termination:** revoke within 30 calendar days of the effective date of the termination action, unless already revoked under Part 5.1 (Part 5.3).
- **Shared accounts:** change passwords for shared accounts known to the user within 30 calendar days of a termination action or of the determination that a transferred user no longer needs the access (Part 5.4).

The 24-hour clock is the one that tests whether HR, security, and operations actually talk to each other. A termination processed on a Friday afternoon is the audit sample you should rehearse.

6.7 Insider Risk Is Reliability Risk

Personnel risk includes the malicious insider, but much of it is ordinary: the technician who keeps access after moving to another plant, the shared administrator password that never changed after a contractor left, the vendor engineer whose remote session was never disabled. CIP-004's controls are built to make human interaction with critical systems predictable and accountable, so that no single person's error or intent goes undetected for long.

6.8 Executive and Engineering Perspectives

For executives, CIP-004 runs across HR, security, contracting, and operations. Its clocks are only met when those groups share one workflow. Staffing and system decisions that leave termination notices sitting in an inbox create direct regulatory exposure.

For engineers and operators, the standard asks for discipline: use your own account, request access through the process, and tell someone when you no longer need it.

Chapter Summary

CIP-004-7 governs the people who can reach high and medium impact systems: quarterly awareness, role-based training before access and every 15 months, seven-year personnel risk assessments, quarterly access verification, and revocation within 24 hours of termination. Chapter 7 turns to the technical protections.

From the Field

Credentials are the shortest path into a control system. CIP's personnel and access requirements are designed around that fact.

A credential that should have been revoked and is still active is the most preventable CIP finding.

The standard expects the quarterly review to find and fix access that should not exist, not just record that it happened.

7 System Security and Technical Protection Concepts

This chapter covers the technical protection standards: CIP-005 (Electronic Security Perimeters), CIP-006 (physical security of BES Cyber Systems), CIP-007 (system security management), CIP-010 (configuration change management and vulnerability assessments), CIP-011 (information protection), CIP-012 (communications between Control Centers), and CIP-013 (supply chain risk management). Technical controls are means, not ends. They exist to keep reliability-critical systems available and operating as intended.

7.1 The Electronic Security Perimeter

CIP-005-7 manages electronic access to BES Cyber Systems through a controlled Electronic Security Perimeter. The ESP is currently defined as the logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol. All External Routable Connectivity must pass through an identified Electronic Access Point, where the entity must require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.

Interactive Remote Access gets its own requirements. For high impact systems and medium impact systems with External Routable Connectivity, CIP-005 requires that all Interactive Remote Access go through an Intermediate System, that the session be encrypted to the Intermediate System, and that it use multi-factor authentication. CIP-005-7 also requires methods to determine active vendor remote access sessions and to disable them.

7.2 Physical Security of BES Cyber Systems

CIP-006-6 requires a physical security plan for high and medium impact systems, with controls that scale by impact and connectivity: Physical Security Perimeters with controlled access, monitoring and alarms for unauthorized entry, logging of entry, and a visitor control program that requires continuous escorted access for visitors. For high impact systems, the entity must use two or more different physical access controls where technically feasible. PACS must be maintained and tested at least once every 24 calendar months.

7.3 System Security Management

CIP-007-6 is the operational core of the technical standards:

- **Ports and services (R1):** where technically feasible, enable only the logical network accessible ports determined to be needed.
- **Patch management (R2):** at least once every 35 calendar days, evaluate security patches released since the last evaluation, and within 35 calendar days of completing the evaluation apply the patch, create a dated mitigation plan, or revise an existing one.

- **Malicious code prevention (R3):** deploy methods to deter, detect, or prevent malicious code.
- **Security event monitoring (R4):** log and alert on security events, and where technically feasible retain applicable logs for at least the last 90 consecutive calendar days for high impact systems and medium impact systems at Control Centers.
- **System access control (R5):** enforce authentication, change known default passwords, enforce password parameters for password-only authentication, and limit, or alert on, unsuccessful authentication attempts.

The 35-day patch cycle never stops. It runs every 35 calendar days for as long as the system is in service, and it produces evidence each cycle. That is why CIP-007 consumes so much operational effort.

7.4 Configuration Change Management and Vulnerability Assessments

CIP-010-4 requires a baseline configuration for each applicable Cyber Asset covering the operating system or firmware, commercially available or open-source software, custom software, logical network accessible ports, and applied security patches. Changes that deviate from the baseline must be authorized and documented, and the baseline must be updated within 30 calendar days of completing the change. Requirement R3 requires a paper or active vulnerability assessment at least once every 15 calendar months, and an active assessment at least once every 36 calendar months for high impact systems where technically feasible. Requirement R4 carries the Transient Cyber Asset and Removable Media protections for high and medium impact systems.

7.5 Information, Communications, and Supply Chain

CIP-011-3 protects BES Cyber System Information: identifying it, protecting it in storage, transit, and use, and preventing unauthorized retrieval when assets that hold it are reused or disposed of.

CIP-012-2, in effect since July 1, 2026, protects the confidentiality, integrity, and availability of Real-time Assessment and Real-time monitoring data transmitted between Control Centers. It applies to Balancing Authorities, Generator Operators, Generator Owners, Reliability Coordinators, Transmission Operators, and Transmission Owners that own or operate a Control Center. The plan must identify methods to mitigate unauthorized disclosure and modification, methods to mitigate loss of the ability to communicate, methods to initiate recovery of the links, and, where Control Centers belong to different entities, each entity's responsibilities.

CIP-013-2 requires a documented supply chain cyber security risk management plan for high and medium impact BES Cyber Systems and their associated EACMS and PACS, its implementation, and CIP Senior Manager or delegate review and approval of the plan at least once every 15 calendar months.

7.6 Controls in Context

None of these controls works alone. A firewall rule set with no change control drifts. A baseline that no one compares against the running configuration goes stale. A patch program without an

asset list misses the devices that matter. The standards are written as separate requirements, but they are implemented as one system of controls, and auditors test them that way.

7.7 Executive and Engineering Perspectives

For executives, the technical standards are where recurring operating cost lives. Patch evaluation, log review, baseline management, and vulnerability assessments are recurring workloads on 35-day, 90-day and 15-month clocks that need staff and tooling, not a one-time project.

For engineers and operators, these standards describe how you change systems: documented, authorized, verified, and recorded. Unplanned change is a reliability risk before it is a compliance risk.

Chapter Summary

The technical CIP standards protect availability and integrity through perimeters, physical controls, system hardening, patching, monitoring, configuration control, vulnerability assessment, information protection, protected inter-control-center communications, and supply chain controls. They work only when integrated with governance and operations. Chapter 8 covers detection, response, and recovery.

> **From the Field**
>
> Technical controls are what the firewall does. They are also what the firewall does not do, and the gaps are usually the audit findings.
>
> CIP-007 and CIP-010 consume most of the operational effort in a CIP program, and with CIP-004 they are the most frequently reported CIP noncompliance. The two facts are connected.
>
> A baseline configuration that was never validated against actual operating need will not survive an audit question. CIP-010 expects validation, not just documentation.

8 Monitoring, Detection, Response, and Recovery Concepts

This chapter covers how CIP addresses the life cycle of a cyber event: seeing it, recognizing it, responding to it, reporting it, and restoring the functions it affected. The standards involved are CIP-007 (event monitoring), CIP-008-6 (incident reporting and response planning), CIP-009-6 (recovery plans), and, from October 1, 2028, CIP-015-1 (internal network security monitoring).

8.1 Cyber Events as Reliability Events

A cyber event does not have to damage equipment to be a reliability event. Loss of visibility, loss of control, or corrupted data in an energy management system can each degrade an operator's ability to keep the system within limits. The Glossary reflects that. A Cyber Security Incident includes a malicious act or suspicious event that disrupts or attempts to disrupt the operation of a BES Cyber System, and, for high or medium impact systems, one that compromises or attempts to compromise an ESP, a Physical Security Perimeter, or an EACMS.

8.2 Monitoring as Situational Awareness

Operators are trained to know what the system is doing in enough detail to act in time. Monitoring a control network is the same discipline applied to the cyber layer. CIP-007 Requirement R4 requires logging and alerting on security events for applicable systems. Good monitoring also catches misconfiguration, failing equipment, and unexpected behavior, which matter to reliability whether or not an attacker is involved.

8.3 Looking Inside the Perimeter

Historically, CIP monitoring concentrated at the perimeter and on individual devices. CIP-015-1 changes that. Its stated purpose is to improve the probability of detecting anomalous or unauthorized network activity to facilitate improved response and recovery. Requirement R1 requires documented processes for internal network security monitoring of networks protected by the ESPs of high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity, starting with network data feeds selected on a risk-based rationale. Requirements R2 and R3 require retention of the monitoring data and protection of it from unauthorized deletion or modification. FERC's Order No. 907 directed NERC to extend the monitoring to EACMS and PACS outside the ESP, which is the subject of CIP-015-2.

8.4 Response and Reporting

CIP-008-6 requires one or more documented Cyber Security Incident response plans for high and medium impact systems and their EACMS. The plans must identify, classify, and respond to incidents, determine which ones are reportable, define roles, and set out incident handling procedures.

Reporting runs on short clocks. A Reportable Cyber Security Incident is one that compromised or disrupted a BES Cyber System that performs reliability tasks, the ESP of a high or medium impact system, or an EACMS of a high or medium impact system. After the entity determines an incident is reportable, it must notify the E-ISAC and, if subject to U.S. jurisdiction, the U.S. National Cybersecurity and Communications Integration Center (NCCIC) or its successor, within one hour. For an incident determined to be an attempt to compromise an applicable system, the deadline is the end of the next calendar day. Updates are due within 7 calendar days of new or changed information on functional impact, attack vector, or level of intrusion.

Response is also an operations activity. Isolating a compromised system may take away an operator's tool at the worst possible time.

8.5 Testing Before the Event

CIP-008 Requirement R2 requires each response plan to be tested at least once every 15 calendar months, by responding to an actual Reportable Cyber Security Incident, by a paper drill or tabletop exercise, or by an operational exercise. Requirement R3 requires the plan to be updated after the test or an actual incident, with communication of the update to the people with roles in the plan, no later than 90 calendar days afterward. The low impact equivalent in CIP-003 Attachment 1 Section 4 requires a test at least every 36 calendar months.

8.6 Recovery

CIP-009-6 requires recovery plans for high and medium impact systems, with conditions for activation, roles, backup and storage of the information needed to recover BES Cyber System functionality, and preservation of data for incident analysis. Requirement R2 requires a test of each recovery plan at least once every 15 calendar months and a test of a representative sample of backup information on the same interval to confirm it is usable and compatible with current configurations. For high impact systems, Requirement R2 adds an operational exercise of the recovery plans at least once every 36 calendar months.

Every test and every real incident should end in a lessons-learned record and a plan update, which the standards require for high and medium impact systems. Treat near misses the same way.

8.7 Executive and Engineering Perspectives

For executives, the one-hour reporting clock means the decision chain for declaring an incident reportable must be settled in advance, with named people available at all hours.

For control room engineers and operators, cyber response plans must speak the language of operations: which displays or controls might be lost, what the fallback is, who calls whom, and how the system is run while a tool is isolated.

Chapter Summary

CIP-007 requires event monitoring, CIP-015 extends monitoring inside the perimeter from 2028, CIP-008 sets one-hour and next-day reporting clocks and 15-month testing, and CIP-009 requires tested recovery plans and usable backups. Chapter 9 covers monitoring and enforcement.

9 CIP Compliance Monitoring and Enforcement

This chapter covers how compliance with the CIP standards is monitored and enforced. It describes the structure and intent of the process, not audit preparation technique, which other references in the series cover.

9.1 Same Program, Same Rules

CIP standards are monitored and enforced under the same statute and the same program as planning, operations, and protection standards. NERC's Compliance Monitoring and Enforcement Program is set out in Appendix 4C to the NERC Rules of Procedure, and NERC and the Regional Entities, acting as Compliance Enforcement Authorities, carry it out. There is no separate CIP enforcement regime.

9.2 How Compliance Is Monitored

Appendix 4C, Section 4.0, lists the monitoring methods: Compliance Audits, Self-Certifications, Spot Checks, Compliance Investigations, Self-Reports, Self-Logging, Periodic Data Submittals, and Complaints. Compliance Audits are risk-based, scheduled under criteria NERC establishes, and may also be initiated unscheduled when the Compliance Enforcement Authority determines it necessary or when FERC directs.

NERC's 2025 annual report shows how the activity mix looks in practice: of CMEP monitoring activities, Self-Certifications accounted for about 87 percent, Compliance Audits about 10 percent, and Spot Checks about 3 percent.

9.3 How a CIP Audit Gathers Evidence

For CIP audits, the Regional Entities use a common CIP Evidence Request Tool. NERC's January 2026 user guide describes a two-level flow. Level 1 asks the entity to complete detail tabs that form populations for sampling, covering BES assets, Cyber Assets, ESPs, Electronic Access Points, PSPs, Transient Cyber Assets, Removable Media, BCSI, personnel, and more, along with the programs and procedures for each standard. Level 2 asks for detailed implementation evidence for the specific items the audit team samples from those populations.

The practical lesson is that the audit is built on your own inventory. If the populations are incomplete, the problem is found in Level 1, before any sample is drawn.

9.4 Risk-Based Oversight

Oversight under the CMEP is risk-based. The ERO Enterprise scales its monitoring to the inherent risk of each registered entity and to the risk a particular noncompliance poses.

9.5 From Noncompliance to Disposition

Appendix 4C, Section 4A, gives the ERO Enterprise enforcement discretion through the Compliance Exception process and the Find, Fix, Track and Report (FFT) process for lower-risk noncompliance. More serious matters proceed through the enforcement actions in Section 5.0: notice of an alleged violation, the entity's response, settlement, and, where needed, a hearing and appeal. Penalties are filed with FERC in a Notice of Penalty under Section 215(e).

In 2025, according to NERC's annual report, the ERO Enterprise processed about 83 percent of filed or submitted noncompliance as Compliance Exceptions and about 14 percent as FFTs, and registered entities self-identified about 85 percent of reported noncompliance.

9.6 Enforcement Follows Noncompliance, Not Incidents

Enforcement is based on violation of a requirement, not on whether an attack occurred. An entity can suffer an incident without violating a standard, and it can violate a standard without ever suffering an incident. The second case is the common one.

9.7 Due Process

The CMEP provides defined rights: notice of alleged violations, an opportunity to respond, settlement procedures, a hearing process, and an appeal to NERC, followed by FERC review of penalties.

9.8 Compliance and Resilience

Compliance with CIP reduces risk. It does not eliminate it, and it does not certify that a system is secure. Resilience depends on more than that: design, staffing, threat intelligence, and the parts of the cyber environment CIP does not reach.

9.9 Executive and Engineering Perspectives

For executives, the CMEP rewards entities that find and fix their own problems. Internal controls that detect noncompliance and a culture that self-reports it are the strongest tools available to manage enforcement exposure.

For engineers and operators, the audit is a technical conversation about systems you run. Records made at the time of the work are worth far more than records reconstructed for the audit.

Chapter Summary

CIP runs through the same risk-based CMEP as every other Reliability Standard, with a common CIP Evidence Request Tool built on sampling. Chapter 10 turns to common misunderstandings.

> **From the Field**
>
> In my experience, CIP audits run denser, with deeper evidence requests and cyber specialists on the team. If you cannot speak the technical language, you end up taking the auditor's framing.

10 Common Misunderstandings About CIP

This chapter addresses the misconceptions that most often distort CIP programs. Each one comes back to scope, purpose, or responsibility.

10.1 CIP Is Not Enterprise Cybersecurity

CIP compliance is not an enterprise-wide cybersecurity program. Its reach is defined by the BES Cyber Asset, BES Cyber System, EACMS, PACS, and PCA definitions and by the statute's limit to the bulk-power system. Enterprise systems that meet none of those definitions are outside CIP.

Folding CIP into a single enterprise framework is fine as a management choice, as long as the CIP scope stays distinct and traceable. When the two blur, the result is either CIP evidence buried in enterprise noise or enterprise priorities distorted by CIP's narrower purpose.

10.2 Compliance Is Not Cybersecurity Maturity

Meeting CIP requirements shows that required controls exist and operate as the standards specify. It does not show that a program is mature, that it addresses every threat to the asset, or that it would stop a capable adversary. The standards are a mandatory baseline for reliability risk. An entity's broader cybersecurity program can and often should go well beyond them.

10.3 CIP Is Not an IT Standard

CIP standards are reliability standards that govern the cybersecurity of operational technology. Handing CIP entirely to an IT group, without operations, engineering, and protection staff in the process, produces controls that do not fit how the systems actually run. The disciplines that need to be in the room are the ones that understand the reliability function the system performs.

10.4 Connectivity Alone Does Not Determine Applicability

Section 3.6 covers why connectivity changes which requirements apply but not whether a device is in scope.

10.5 CIP Does Not Eliminate Cyber Risk

CIP reduces specific risks to specific systems. It does not remove every threat or vulnerability, and the standards themselves keep changing as the threat changes. Compliance does not equal zero risk.

10.6 Enforcement Is Not Triggered by Incidents

An incident may bring scrutiny that reveals a violation. Section 9.6 explains why the violation, not the incident, is what gets enforced.

10.7 CIP Is Not Static

The CIP family is revised through the standards development process to address lessons learned, new technology, and new threats. Since 2016 the low impact program, incident reporting, supply chain, inter-control-center communications, and vendor remote access have all been added or tightened, and internal network security monitoring and virtualization are scheduled for 2028. A program designed once and left alone falls out of compliance on its own.

10.8 Responsibility Is Broader Than One Team

CIP responsibility does not belong only to IT, security, or compliance. Operations, engineering, procurement, HR, and management decisions all affect CIP scope and risk. Procurement decisions touch CIP-013. HR decisions start the CIP-004 revocation clocks. Engineering changes trigger CIP-010. Each function needs to know where its decisions touch the standards.

10.9 CIP Is Part of the Reliability System

CIP is one part of a larger reliability framework that also covers planning, operations, protection, and governance. A protection engineer's relay settings and a CIP-010 baseline for the same relay are two views of the same equipment. Programs work best when they are managed that way.

Chapter Summary

Most CIP misunderstandings come down to scope, purpose, or responsibility. CIP is a reliability standard family with a defined scope, a minimum baseline, and shared organizational ownership. Clearing those misconceptions early makes the rest of the program easier to build. Chapter 11 helps an organization find its place in the framework.

> **From the Field**
>
> "We outsourced cybersecurity to the IT vendor" is not a CIP defense. The registered entity is accountable, regardless of whom it contracted with.
>
> "We are CIP-compliant because we passed the audit" produces the next finding. An audit tests a sample on the day it happens; the program has to run every day in between.
>
> Programs that frame CIP as an IT problem tend to staff it from IT alone. Staff it as a reliability problem with IT controls, with operations and engineering at the table.

11 Getting Oriented Within the CIP Framework

This chapter helps an organization locate itself in the CIP framework: how it comes into scope, how applicability changes over time, and how CIP responsibility fits into its broader reliability program. It does not cover implementation of individual requirements.

11.1 Entry Points

Most organizations meet CIP through registration. An entity registered as a Balancing Authority, Generator Owner, Generator Operator, Reliability Coordinator, Transmission Operator, Transmission Owner, or a Distribution Provider with in-scope equipment becomes a Responsible Entity under CIP-002. Registration criteria are set in Appendix 5B to the NERC Rules of Procedure, the Statement of Compliance Registry Criteria.

Scope can also change without a new registration. New generation or an uprate can cross the 1500 MW line. A new 500 kV interconnection can create a medium impact substation. A Planning Coordinator or Transmission Planner designation under criterion 2.3, or a Reliability Coordinator's identification of a Facility as critical to IROLs under criterion 2.6, can change an asset's rating. A new fleet control center can change the Generator Operator criteria that apply.

11.2 Applicability Changes Over Time

Applicability is not a one-time determination. It reflects the current system and the current configuration, which is why CIP-002 requires a review and CIP Senior Manager approval at least every 15 calendar months. Build the triggers into change management, interconnection, and project processes so that the CIP team hears about the change before the asset goes in service, not at the next 15-month review.

11.3 Organizational Alignment

CIP reaches across operations, engineering, planning, IT, security, HR, procurement, and governance. Individual tasks can be assigned to individuals, but the Responsible Entity is accountable for all of them, and CIP-003 makes the CIP Senior Manager the single person with overall authority. A responsibility matrix that maps each requirement to an owning function is one of the first documents a new CIP program should produce.

11.4 Governance and Oversight

Executive oversight does not require technical expertise. It requires informed questions. How many BES Cyber Systems do we have at each impact level? What changed in our scope this year? Who is our CIP Senior Manager and what authority do they hold? What did our last

incident response test show? Where are we relying on a vendor for remote access, and how is that controlled?

11.5 Working With Oversight Bodies

Once in scope, an entity works with its Regional Entity through audits, self-certifications, spot checks, and self-reports. Regional Entities also run outreach, workshops, and compliance assistance. Use them. A relationship built on transparent self-reporting and timely responses makes every monitoring activity more efficient for both sides.

11.6 CIP as an Ongoing Responsibility

CIP is never finished. Systems change, standards change, and the threat changes. New automation, communications, and control technology can move what counts as a BES Cyber Asset. Sustained attention, built into normal operations, is the only approach that keeps up.

11.7 Avoiding Early Misconceptions

Organizations new to CIP often treat it as a paperwork exercise or as an irritating technical burden. Treat it instead as a structured way to manage one category of reliability risk, with compliance records as the evidence that the management is happening.

11.8 Executive and Engineering Perspectives

For executive leaders, orientation means understanding the entity's CIP footprint, the decisions that change it, and the accountability structure that governs it.

For engineers and operations staff, orientation means knowing which systems are in scope, which procedures apply to them, and how cyber controls connect to the commissioning, maintenance, and operating work they already do.

Chapter Summary

Getting oriented to CIP starts with registration, the impact criteria, and a clear map of who is responsible for what. Scope changes as the system changes, so the triggers belong inside normal business processes. Chapter 12 draws the main themes of this reference together.

12 Executive and Engineering Takeaways

This chapter brings together the main themes of CIP 101 for executives, engineers, and senior management.

12.1 Cybersecurity Is a Reliability Discipline

Section 215 treats cybersecurity protection as part of reliable operation, and CIP standards are enforced like every other Reliability Standard. Cyber Assets that monitor, control, or protect the BES deserve the same engineering discipline as the equipment they serve.

12.2 Governance Shapes Outcomes

Many of the choices that create CIP risk are governance choices: organizational design, policies and procedures, architecture, staffing, and vendor relationships. The table below gives examples.

Area of choice	Example decision	CIP consequence
Organizational design	Who is named CIP Senior Manager and what authority they hold	Accountability under CIP-003 R3; approvals under CIP-002 R2 and CIP-003 R1
Policies and procedures	Whether HR terminations feed security in real time	The 24-hour revocation clock in CIP-004 R5
System architecture	Adding routable remote access to a medium impact system	External Routable Connectivity switches on CIP-004 and CIP-005 IRA requirements
Resourcing	Staffing the 35-day patch evaluation cycle	The 35-day cycles in CIP-007 R2
Vendors	Allowing vendor remote access to a low impact site	CIP-003-9 Attachment 1, Section 6

Executives cannot hand cyber reliability to the technical teams and walk away. Executive decisions create the conditions those teams work in.

12.3 Engineering Judgment Remains Central

The CIP standards set mandatory requirements, but most of them leave method to the entity: how to group BES Cyber Systems, which ports are needed, which monitoring feeds to use under CIP-015's risk-based rationale. Those are engineering judgments. Document the reasoning when you make them, because the auditor will ask.

12.4 Compliance Supports but Does Not Define Reliability

Meeting the CIP requirements is the minimum. Other risks in the organization, the system, or the threat environment can affect reliability regardless of compliance status. There is always more a program can do, and in my view the best programs decide deliberately where to go beyond the floor.

12.5 Integration Across Disciplines

CIP touches operations, engineering, planning, procurement, HR, and governance. Siloed programs develop blind spots at the boundaries between those groups, which is where revocation, change management, and scope failures tend to start.

12.6 Oversight as a Supporting Function

Compliance monitoring and enforcement promote accountability and consistency. They do not prescribe engineering solutions or replace the entity's judgment. An entity that understands that can engage oversight as a check on its own controls rather than as an adversary.

12.7 Adaptation and Evolution

The CIP framework will keep changing as technology, architectures, and threats change. That is a feature of the framework, not a weakness. The 2028 virtualization and internal network security monitoring dates are close enough to plan for now.

12.8 Shared Responsibility

The BES is interconnected. One entity's weakness can affect its neighbors, its Reliability Coordinator, and the systems it exchanges data with. CIP-012's requirements for protecting data between Control Centers owned by different entities are a direct expression of that shared responsibility.

Chapter Summary

The NERC CIP standards apply reliability discipline to the digital systems the grid now depends on. Governance, engineering judgment, and coordination across the organization determine whether a CIP program protects reliability or only produces evidence. This reference is the foundation for the rest of the CIP series, which takes each standard in depth.

Glossary

Terms in this glossary are defined in the NERC Glossary of Terms Used in Reliability Standards unless noted. The definitions below are the versions subject to enforcement as of October 2026; several are revised effective July 1, 2028 under the Project 2016-02 virtualization changes. Consult the current NERC Glossary for authoritative text.

Term	Meaning in this paper
BES Cyber Asset	A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, 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. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.
BES Cyber System	One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.
Bulk Electric System (BES)	Unless modified by the inclusions and exclusions in the NERC Glossary, all Transmission Elements operated at 100 kV or higher and Real Power and Reactive Power resources connected at 100 kV or higher. It does not include facilities used in the local distribution of electric energy.
CIP Exceptional Circumstance	A situation that involves or threatens to involve one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death; a natural disaster; civil unrest; an imminent or existing hardware, software, or equipment failure; a Cyber Security Incident requiring emergency assistance; a response by emergency services; the enactment of a mutual assistance agreement; or an impediment of large scale workforce availability.
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, CIP-002 through CIP-011.
Critical Cyber Asset	Historical term from CIP Version 1 through Version 3 for a Cyber Asset essential to the reliable operation of a Critical Asset. Retired with the Version 5 standards approved in FERC Order No. 791 (not a current Glossary term).
Cyber Assets	Programmable electronic devices, including the hardware, software, and data in those devices.
Cyber Security Incident	A malicious act or suspicious event that, for a high or medium impact BES Cyber System, compromises or attempts to compromise an Electronic Security Perimeter, a Physical Security Perimeter, or an Electronic Access Control or Monitoring System; or disrupts or attempts to disrupt the operation of a BES Cyber System.

Term	Meaning in this paper
Electronic Access Control or Monitoring Systems (EACMS)	Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems.
Electronic Security Perimeter (ESP)	The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.
External Routable Connectivity	The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection.
Impact rating	As used in this reference, the High, Medium, or Low categorization of a BES Cyber System under CIP-002 Attachment 1 (not a Glossary term).
Interactive Remote Access	User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol, originating from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeters or at a defined Electronic Access Point. It does not include system-to-system process communications.
Intermediate System	A Cyber Asset or collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users. The Intermediate System must not be located inside the Electronic Security Perimeter.
Physical Access Control Systems (PACS)	Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.
Physical Security Perimeter (PSP)	The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.
Protected Cyber Assets (PCA)	One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP.
Reportable Cyber Security Incident	A Cyber Security Incident that compromised or disrupted a BES Cyber System that performs one or more reliability tasks of a functional entity; an Electronic Security Perimeter of a high or medium impact BES Cyber System; or an Electronic Access Control or Monitoring System of a high or medium impact BES Cyber System.

How Energy Compliance Can Help

CIP programs fail at the gate more often than at the firewall. EC works where scope, governance, and evidence meet.

Scope and categorization

CIP applicability and scope analysis (CIP-002 through CIP-014); Cyber Asset and BES Cyber System identification and impact classification; Electronic Security Perimeter and Physical Security Perimeter boundary analysis; registration and applicability analysis when a facility, uprate, or control center changes the picture.

Program, audit, and enforcement

CIP governance and program assessments; CIP framework reviews, gap analyses, and improvement plans; integration of cybersecurity oversight with broader reliability programs; NERC compliance program support, interpretation, and audit preparation; compliance program management; RSAW production and data request strategy; audit and enforcement support for CIP findings (non-advocacy); audit defense, including Notice of Penalty response and settlement posture.

Advisory and training

Senior advisory engagement on complex reliability questions; training focused on the CIP framework, requirements, and audit expectations; executive and board-level CIP awareness briefings; industry engagement in standards development and working-group participation. Services are tailored to each organization's functional role, system impact, and regulatory posture.

WattOps Compliance and RenewOps

WattOps Compliance is EC's NERC compliance evidence platform (wattopscompliance.com), for the O&P evidence that sits beside a CIP program. EC will run one standard at one facility through WattOps at no cost (CIP standards excluded). RenewOps is EC's renewable operations monitoring and analytics platform, with a Data Center module, for the plant and SCADA data that CIP-002 scope decisions start from.

If you are not certain your CIP-002 categorization would survive an audit question today, start there.

Website: energycomplianceinc.com · Email: rsmith@complianceforenergy.com

Phone: 763.438.4427

About the Author

Rob Smith is the Founder and Principal of Energy Compliance, Inc., with more than thirty years in the industry on every side of the system. He began in control-room operations as a Reliability Coordinator, Transmission Operator, and Power System Operator across RTO/ISO and utility control centers. On the regulator side, he was a senior compliance auditor and subject matter expert for NERC Reliability Standards. He audited grid facilities, evaluated mitigation adequacy, participated in risk-based oversight of utility mitigation activities, and supported the development of violation notifications and settlements in FERC-directed enforcement actions. He conducted a regulatory audit in the Sultanate of Oman against the Sultanate's Sector Law and Grid Code.

He founded Energy Compliance, Inc. to deliver senior regulator-side compliance authority without the layered staffing and billable-hour overhead of larger firms.

Education:

- MBA, Energy Management, University of Mary
- MSL, Compliance Law, Fordham Law University
- BAS, Energy Management, Bismarck State College
- BAS, Mechanical Engineering, Metallurgy minor, University of Florida
- BAS, Criminology, St. Petersburg College (State Law Enforcement Certification)
- AAS, Power Plant Technology, Bismarck State College
- AAS, Electrical Transmission System Technology, Bismarck State College

Certifications: NERC Lead Auditor training; previously NERC-certified at the Reliability Coordinator level; 1st Class A Boiler Engineer License, Minnesota.

About Energy Compliance, Inc.

Energy Compliance, Inc. is an independent consulting and advisory firm based in Bloomington, Minnesota, focused exclusively on electric reliability, cybersecurity reliability, and regulatory compliance for organizations connected to the North American Bulk Electric System.

We support registered entities, including Generator Owners and Operators, Transmission Owners and Operators, Reliability Coordinators, Balancing Authorities, and Distribution Providers. Our work spans NERC Reliability Standards, FERC orders, RTO/ISO market participation rules, Regional Entity oversight, and state regulatory frameworks.

We do this work differently than larger consulting firms. A senior practitioner with regulator-side experience oversees every engagement. We staff for outcomes, not billable hours. Our deliverables are written to be operationally executable and audit-defensible, structured for the auditor's question rather than the consultant's binder. Where automation can replace manual work, we build the automation. Where senior judgment is required, the senior is in the room.

Energy Compliance is not affiliated with, sponsored by, or endorsed by the North American Electric Reliability Corporation, the Federal Energy Regulatory Commission, or any Regional Entity.

Learn more at energycomplianceinc.com.

Sources and Authorities

- Federal Power Act § 215, 16 U.S.C. § 824o, Electric reliability. https://www.law.cornell.edu/uscode/text/16/824o
- Federal Energy Regulatory Commission, Order No. 706, Mandatory Reliability Standards for Critical Infrastructure Protection, Docket No. RM06-22-000 (issued January 18, 2008), 73 FR 7368 (February 7, 2008). https://www.govinfo.gov/link/fr/73/7402
- Federal Energy Regulatory Commission, Order No. 791, Version 5 Critical Infrastructure Protection Reliability Standards, Docket No. RM13-5-000 (issued November 22, 2013), 78 FR 72756 (December 3, 2013). https://www.govinfo.gov/content/pkg/FR-2013-12-03/pdf/2013-28628.pdf
- Federal Energy Regulatory Commission, Order No. 907, Critical Infrastructure Protection Reliability Standard CIP-015-1, Cyber Security, Internal Network Security Monitoring, Docket No. RM24-7-000 (issued June 26, 2025), 90 FR 28889 (July 2, 2025). https://www.govinfo.gov/content/pkg/FR-2025-07-02/html/2025-12309.htm
- U.S.-Canada Power System Outage Task Force, Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations (April 2004). https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf
- North American Electric Reliability Corporation, Reliability Standards, CIP family listing (retrieved October 26, 2026). https://www.nerc.com/standards/reliability-standards/cip
- NERC Reliability Standard CIP-002-5.1a, Cyber Security, BES Cyber System Categorization. https://www.nerc.com/globalassets/standards/reliability-standards/cip/cip-002-5.1a.pdf
- NERC Reliability Standard CIP-003-9, Cyber Security, Security Management Controls (effective April 1, 2026). https://www.nerc.com/globalassets/standards/reliability-standards/cip/cip-003-9.pdf
- NERC Reliability Standard CIP-004-7, Cyber Security, Personnel & Training. https://www.nerc.com/globalassets/standards/reliability-standards/cip/cip-004-7.pdf
- NERC Reliability Standard CIP-005-7, Cyber Security, Electronic Security Perimeter(s). https://www.nerc.com/globalassets/standards/reliability-standards/cip/cip-005-7.pdf
- NERC Reliability Standard CIP-006-6, Cyber Security, Physical Security of BES Cyber Systems. https://www.nerc.com/globalassets/standards/reliability-standards/cip/cip-006-6.pdf

- NERC Reliability Standard CIP-007-6, Cyber Security, System Security Management. https://www.nerc.com/globalassets/standards/reliability-standards/cip/cip-007-6.pdf
- NERC Reliability Standard CIP-008-6, Cyber Security, Incident Reporting and Response Planning. https://www.nerc.com/globalassets/standards/reliability-standards/cip/cip-008-6.pdf
- NERC Reliability Standard CIP-009-6, Cyber Security, Recovery Plans for BES Cyber Systems. https://www.nerc.com/globalassets/standards/reliability-standards/cip/cip-009-6.pdf
- NERC Reliability Standard CIP-010-4, Cyber Security, Configuration Change Management and Vulnerability Assessments. https://www.nerc.com/globalassets/standards/reliability-standards/cip/cip-010-4.pdf
- NERC Reliability Standard CIP-011-3, Cyber Security, Information Protection. https://www.nerc.com/globalassets/standards/reliability-standards/cip/cip-011-3.pdf
- NERC Reliability Standard CIP-012-2, Cyber Security, Communications between Control Centers (effective July 1, 2026). https://www.nerc.com/globalassets/standards/reliability-standards/cip/cip-012-2.pdf
- NERC Reliability Standard CIP-013-2, Cyber Security, Supply Chain Risk Management. https://www.nerc.com/globalassets/standards/reliability-standards/cip/cip-013-2.pdf
- NERC Reliability Standard CIP-014-3, Physical Security. https://www.nerc.com/globalassets/standards/reliability-standards/cip/cip-014-3.pdf
- NERC Reliability Standard CIP-015-1, Cyber Security, Internal Network Security Monitoring (effective October 1, 2028). https://www.nerc.com/globalassets/standards/reliability-standards/cip/cip-015-1.pdf
- NERC, Glossary of Terms Used in NERC Reliability Standards (web version, retrieved October 25, 2026). https://www.nerc.com/glossary-of-terms
- NERC Rules of Procedure, Appendix 4C, Compliance Monitoring and Enforcement Program (effective May 19, 2022). https://www.nerc.com/globalassets/who-we-are/rules-of-procedure/appendix-4c.pdf
- NERC Rules of Procedure, Appendix 5B, Statement of Compliance Registry Criteria (Revision 8, effective June 27, 2024). https://www.nerc.com/globalassets/who-we-are/rules-of-procedure/appendix-5b.pdf
- NERC, ORCP and CMEP Annual Report (February 11, 2026), covering 2025. https://www.nerc.com/globalassets/programs/enforcement/cmep-and-vegetation-reports/2025-orcp-and-cmep-annual-report.pdf
- NERC, ERO Enterprise Critical Infrastructure Protection Evidence Request Tool User Guide (January 2026). https://www.nerc.com/globalassets/programs/compliance/cmep-resources/cip-evidence-request-tool-user-guide-v10.pdf
- NERC, Reliability Standards Compliance Dates for Generator Owners and Generator Operators, Inverter-Based Resource Registration Initiative Supplemental (Revision 1.5, August 4, 2026). https://nerc.com/pa/Stand/202401%20Rules%20of%20Procedure%20Definitions%20Alignment%20GO/ComplianceDatesforGOs_GOPS.pdf

© Energy Compliance, Inc. · EC-WP-200 · October 2026