CYBERSECURITY · CIP SERIES · EC-WP-201

CIP Low & Medium Impact

What Low and Medium Impact mean, why the categories exist, and how they shape compliance programs.

Every CIP program starts with one decision under CIP-002, and that decision sets every obligation that follows. This reference explains what the low and medium impact ratings mean, what each one triggers, and where programs most often go wrong. It covers the requirements in force in October 2026 and the changes already approved for 2028 and 2029.

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 regulatory citations in this edition were checked against the primary sources listed in Sources and Authorities as of October 2026. Standards change. Confirm the current version before relying on any requirement described here.

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

The entities that do reliability well share a common habit. They take the standards seriously without confusing them with reliability itself. They know that a NERC Reliability Standard is a floor, not a ceiling. They know that compliance is something an auditor evaluates, but reliability is something a system either delivers or doesn't. They prepare for audits by building programs that survive real questions, not binders that look thick.

That's the perspective these references try to share. Each one focuses on a single topic: a standard family, an operational function, a regulatory framework, or an emerging industry challenge. Each one walks through how the topic actually works.

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

same thing and suspects they aren't. And for the new compliance hire who got handed a binder and told good luck.

These references aren't marketing material disguised as content. They're the result of three decades of doing this work and watching it succeed and fail. I've written them in the same voice I use in a control room or in front of a Regional Entity audit team: direct, evidence-grounded, honest about what the standards do and do not require.

Energy Compliance exists because most 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 don't bring five people to a meeting that needs one. We automate the work that should be automated. We apply senior judgment to the work that requires it. If that approach matches what you're looking for in a compliance partner, the back of this reference has our contact information.

If not, the reference still belongs to you. Take what's useful. 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

CIP-002 sorts every BES Cyber System into one of three impact ratings: high, medium, or low. High impact is narrow. Under Attachment 1 of CIP-002-5.1a it reaches only certain Control Centers and backup Control Centers of Reliability Coordinators, Balancing Authorities, Transmission Operators, and Generator Operators. That means every BES Cyber System serving a generating plant, a substation, or a field location, other than a qualifying Control Center, is medium impact at most, and anything at an in-scope asset that misses the high and medium criteria lands in low impact by default. For most of the people who run CIP programs day to day, the low and medium tiers are the program.

In my view, treating either tier as a lesser obligation is one of the most common errors in CIP practice. Low impact carries its own enforceable plan under CIP-003-9, which became effective on April 1, 2026 and added vendor electronic remote access controls. Medium impact pulls in most of the CIP family, from personnel and training through supply chain risk management. FERC approved further low impact controls in Order No. 918 in March 2026, citing the risk of a coordinated attack on low impact facilities whose aggregate impact could be much greater.

The points below are my own read of where programs succeed and fail. Each is developed, with its sources, in the chapters that follow.

- "Low impact" doesn't mean low importance, and it doesn't mean unregulated or unaudited.
- Categorization errors rarely show at registration. They show at the next audit, after the program was built around the wrong scope. NERC's 2025 annual report puts CIP-002 on its list of the ten most frequently reported CIP noncompliance areas.
- Medium impact requirements run deeper than low because the consequence of compromise is higher. The rating changes the control architecture, not just the paperwork.
- Electronic and Physical Security Perimeters, which apply to medium and high impact systems, get drawn once and rarely re-checked. Problems cluster in the gap between the drawn boundary and the actual one.
- A low impact program scaled up doesn't become a medium impact program. Different obligations, different evidence expectations.
- Governance scales with consequence. Light governance on medium impact is a finding waiting for a trigger.
- The requirements are moving. Virtualization revisions across the CIP family take effect July 1, 2028, and CIP-003-11 adds low impact authentication and detection controls on July 1, 2029.

1 Why Low and Medium Impact Matter in the CIP Framework

The CIP standards exist to protect the cyber systems that operate and support the Bulk Electric System. They do not protect every system equally, and they were never meant to. This chapter explains why the framework sorts systems by impact, why the low and medium tiers carry most of the day-to-day work, and why a lower rating never means a lighter sense of responsibility.

1.1 Impact Classification as a Reliability Concept

CIP-002 states its own purpose plainly: to identify and categorize BES Cyber Systems and their associated BES Cyber Assets "for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES." The operative word is commensurate. The rating is a statement about consequence. It says how much harm to the Bulk Electric System a compromised system could do. It says nothing about how likely an attack is, how valuable the equipment is, or how hard the system is to defend.

That distinction matters because the same attacker, using the same technique, could reach a low impact relay panel as easily as a medium impact control system. Likelihood does not drive the rating. Consequence does, and the rating then drives which requirements apply.

1.2 Three Ratings, Not Four

Attachment 1 of CIP-002-5.1a defines three ratings and only three:

- **High impact (Section 1).** BES Cyber Systems used by and located at certain Control Centers and backup Control Centers: every Reliability Coordinator Control Center, and Balancing Authority, Transmission Operator, and Generator Operator Control Centers that meet the size or asset tests in criteria 1.2 through 1.4.
- **Medium impact (Section 2).** BES Cyber Systems not already rated high that are associated with the facilities in criteria 2.1 through 2.13, such as large generating plants, high-voltage transmission stations, IROL-critical facilities, and larger Control Centers.
- **Low impact (Section 3).** BES Cyber Systems not included in Sections 1 or 2 that are associated with Control Centers, transmission stations and substations, generation resources, restoration facilities including Blackstart Resources and Cranking Paths, Special Protection Systems, and certain Distribution Provider Protection Systems.

There is no "non-critical" category for a BES Cyber System at an in-scope asset. If the system meets the definition and the asset is in scope, it carries a rating.

1.3 Where Most Programs Actually Live

Because Section 1 reaches only Control Centers, every BES Cyber System at a power plant or substation, other than a qualifying Control Center, is rated medium or low. Section 3 then works as the default: an in-scope asset that does not trip a high or medium criterion still contains low impact BES Cyber Systems. A wind farm, a solar plant, a battery site, or a 138 kV switching station can all land there.

That is why low impact cannot be treated as an afterthought. For many registered entities it is the entire CIP program. In my view, for nearly all of them it covers the largest number of assets.

1.4 Regulatory Intent Behind Impact Differentiation

Applying high impact controls to every relay and plant controller would impose heavy cost for little reliability benefit. Applying nothing would leave the grid exposed through its most numerous assets. The tiered model sits between those two failures. Controls scale with the consequence of compromise.

FERC has made clear that the low tier is not where risk disappears. In Order No. 918, issued March 19, 2026, the Commission approved CIP-003-11 to address the risk of a "coordinated cyberattack on low-impact facilities, the aggregate impact of which could be much greater." One low impact site is a local problem. Fifty of them compromised at once is a different problem, and the standards are moving to reflect it.

1.5 What This Means for Executives and Engineers

For executives

Impact classification tells leadership where cyber risk to reliability sits and how much control the standards demand at each location. Getting it right keeps cybersecurity spending proportional. Getting it wrong either wastes money on controls the system does not need or leaves an enforceable gap that will surface at audit.

For engineers and operators

The rating ties a system's function to its reliability consequence. Two devices that look identical on the bench can carry different ratings because of where they sit and what they control. Understanding why a system is rated the way it is makes the controls that follow easier to apply and easier to defend.

> **From the Field**
>
> Low impact does not mean low importance. It means a different proportionality of controls. In my view, treating low impact as unregulated is one of the most common routes to a finding.
>
> The rating follows the Attachment 1 criteria, not the nameplate. Two plants of similar size can carry different ratings if a Planning Coordinator designates one of them under criterion 2.3, and that rating drives every requirement that follows.

2 Defining Low Impact and Medium Impact Systems

Classification is not a matter of interpretation or preference. It follows defined terms, a required process, and threshold criteria. This chapter walks through each, then looks at the definitional changes already approved for 2028.

2.1 The Building Blocks: Cyber Asset, BES Cyber Asset, BES Cyber System

Three NERC Glossary terms do most of the work.

- A **Cyber Asset** is a programmable electronic device, including the hardware, software, and data in it.
- A **BES Cyber Asset** is 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 that would affect the reliable operation of the Bulk Electric System. Redundancy is not considered when determining adverse impact.
- A **BES Cyber System** is one or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.

The rating attaches to the BES Cyber System, not to the individual device. The 15-minute test and the "redundancy is not considered" clause are where most scoping arguments start.

2.2 The CIP-002 Process

CIP-002-5.1a applies to Balancing Authorities, certain Distribution Providers, Generator Operators, Generator Owners, Interchange Coordinators or Interchange Authorities, Reliability Coordinators, Transmission Operators, and Transmission Owners. Requirement R1 obliges each of them to implement a process that considers six asset types: Control Centers and backup Control Centers; transmission stations and substations; generation resources; systems and facilities critical to system restoration; Special Protection Systems; and, for Distribution Providers, specified Protection Systems.

From that process the entity must:

- identify each high impact BES Cyber System (R1.1);
- identify each medium impact BES Cyber System (R1.2); and
- identify each asset that contains a low impact BES Cyber System (R1.3). A discrete list of low impact BES Cyber Systems is not required.

Requirement R2 then requires the entity to review and update those identifications at least once every 15 calendar months, and to have its CIP Senior Manager or delegate approve them on the same cycle, even if nothing was identified.

2.3 Medium Impact Criteria at a Glance

The medium impact criteria are specific and mostly quantitative.

Criterion	What it captures
2.1	Generation at a single plant location of 1,500 MW or more in a single Interconnection (only the shared BES Cyber Systems that could affect units totaling 1,500 MW within 15 minutes)
2.2	Reactive resources at a single location of 1,000 MVAR or more, excluding generation Facilities
2.3	Generation a Planning Coordinator or Transmission Planner designates as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year
2.4	Transmission Facilities operated at 500 kV or higher
2.5	200 kV to 499 kV stations connected to three or more other stations with an aggregate weighted value above 3,000
2.6	Generation or Transmission Facilities identified as critical to the derivation of IROLs
2.7	Transmission Facilities essential to Nuclear Plant Interface Requirements
2.8	Interconnection Facilities whose loss would lose generation identified under 2.1 or 2.3
2.9	SPS, RAS, or automated switching whose failure would cause or reduce IROLs
2.10	Automatic UFLS or UVLS of 300 MW or more under a common control system
2.11	Generator Operator Control Centers for 1,500 MW or more in a single Interconnection
2.12	Transmission Operator Control Centers not rated high
2.13	Balancing Authority Control Centers for 1,500 MW or more in a single Interconnection

Anything associated with a Section 3 asset that falls outside these criteria is low impact.

2.4 Functional Role as the Primary Driver

The criteria turn on what a facility does for the system: the MW it can deliver, the voltage it operates at, whether it is critical to an IROL, whether its loss would strand designated generation. The technology inside the cabinet does not change the rating, and neither does the business unit that owns it. A plant controller performing the same reliability function at two similar plants should be categorized the same way, unless a criterion such as 2.3 applies to one and not the other.

2.5 Avoiding Misclassification Through Overgeneralization

A common mistake is to treat classification as a site-wide label. Ratings attach to BES Cyber Systems. A single generating plant can hold medium impact shared systems under criterion 2.1 and low impact systems for individual units that cannot reach the 1,500 MW threshold. A Control Center rating does not carry down to the field assets it monitors.

Associated systems matter too. NERC's 2025 annual report explains that no current CIP standard contains a stand-alone requirement to identify Physical Access Control Systems, Protected Cyber Assets, or Electronic Access Control or Monitoring Systems. When an entity misses one, the ERO Enterprise rolls the resulting noncompliance into a single CIP-010 R1 violation while a permanent fix is developed under Project 2021-03. Scoping errors do not always show up under CIP-002. They often show up somewhere else.

2.6 Changes Already Approved

The definitions are not standing still.

- **Virtualization (July 1, 2028).** FERC approved the Project 2016-02 virtualization standards in Docket No. RM24-8-000. The revised definitions, including BES Cyber Asset, Cyber Assets, and Electronic Security Perimeter, become effective July 1, 2028. CIP-002-8 (FERC Docket No. RD25-8-000) takes effect the same day and supersedes CIP-002-7, which is retired immediately before CIP-002-8 takes effect.
- **Control Centers and criterion 2.12 (CIP-002-8).** On March 19, 2026, FERC approved CIP-002-8 in Docket No. RD25-8-000. The revised Control Center definition reaches a Transmission Owner that can control transmission Facilities at two or more locations using SCADA. Criterion 2.12 will use a weighted value of transmission lines monitored and controlled, with a threshold of 6,000 and an exclusion for local systems that mainly serve load. NERC lists CIP-002-8 as effective July 1, 2028.
- **Category 2 inverter-based resources.** NERC's compliance dates document for newly registered Category 2 IBR Generator Owners and Generator Operators (Revision 1.5, August 4, 2026) shows CIP-002 through CIP-013 and CIP-015 as "requires modification" before they become applicable to Category 2 IBRs. A Category 2 registrant should track that list rather than assume CIP applies or does not.

For executives

The definitions decide the scope of the whole program. A change in a definition is a change in scope, and two of them are scheduled for 2028.

For engineers and operators

Knowing the 15-minute test and the criteria lets you explain, in writing, why each system carries the rating it does. That written rationale is what an audit team will ask for first.

> **From the Field**
>
> A BES Cyber System is what the standard regulates. The asset inventory is what proves the scope. The two have to reconcile, in writing, before audit.

3 Low Impact CIP: Reliability Context and Oversight Intent

Low impact requirements live almost entirely in CIP-003-9, Security Management Controls, which became mandatory on April 1, 2026. The structure is simple to describe and harder to execute well: a policy, a plan, a named senior manager, and six defined plan sections. This chapter covers each and the changes already approved.

3.1 The Role of Low Impact Systems in Reliability

Low impact BES Cyber Systems control, monitor, or protect equipment at individual facilities: plant controllers, substation automation, protective relays with routable communications, and the networks that connect them. A single compromise usually has a local effect. The concern FERC described in Order No. 918 is aggregation. Many similar low impact sites, reached the same way, could produce an effect no single site could.

3.2 Policy, Senior Manager, and Delegation

CIP-003-9 sets four requirements.

- **R1.2, policy.** For assets containing low impact BES Cyber Systems, one or more documented cyber security policies covering seven topics: 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 declaring and responding to CIP Exceptional Circumstances. The CIP Senior Manager must review and approve the policies at least once every 15 calendar months.
- **R2, plan.** An entity with at least one asset containing low impact BES Cyber Systems must implement one or more documented cyber security plans that include the sections in Attachment 1.
- **R3, CIP Senior Manager.** The entity must identify its CIP Senior Manager by name and document any change within 30 calendar days.
- **R4, delegation.** If the CIP Senior Manager delegates authority, the delegations must be documented, approved, and updated within 30 days of any change.

3.3 The Six Sections of the Low Impact Plan

Attachment 1 of CIP-003-9 defines what the plan must contain.

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 BES Cyber Systems within it, and to any Cyber Assets that provide the electronic access controls under Section 3.1.
3. **Electronic access controls.** Permit only necessary inbound and outbound electronic access for communications that are between a low impact BES Cyber System and a Cyber Asset outside the asset, use a routable protocol when entering or leaving the asset, and are not used for time-sensitive protection or control functions between intelligent electronic devices. Authenticate all Dial-up Connectivity, per Cyber Asset capability.
4. **Cyber Security Incident response.** One or more plans covering identification, classification, and response; determination of reportability and notification to the E-ISAC; roles and responsibilities; incident handling; testing at least once every 36 calendar months; and updates, if needed, within 180 calendar days after a test or an actual Reportable Cyber Security Incident.
5. **Transient Cyber Assets and Removable Media.** A plan to mitigate the risk of malicious code from laptops and media, with specific methods for entity-managed devices, third-party devices, and Removable Media.
6. **Vendor electronic remote access.** For assets that allow vendor electronic remote access, methods for determining that access, disabling it, and detecting known or suspected malicious communications. Section 6 is new in CIP-003-9.

3.4 Proportionality and the Asset-Level View

Low impact compliance is organized by asset, not by device. CIP-002 R1.3 requires a list of assets containing low impact BES Cyber Systems and says a discrete list of the systems is not required. CIP-003 lets an entity build a plan by individual asset or by groups of assets, and lets entities with higher-rated systems reuse their high or medium impact policies and procedures to satisfy the low impact sections.

That is proportionality in practice. The standard asks whether the protections exist at each asset, not whether every device has its own record.

3.5 Avoiding Overextension of Low Impact Scope

The opposite error also happens. Some programs treat low impact requirements as enterprise-wide IT controls and pull corporate systems into the plan. That adds work without adding reliability benefit and can blur the evidence trail an audit team needs to follow. In my view, the cleanest low impact programs are the ones that can draw a clear line around each asset, show what crosses that line, and show the controls on it.

3.6 Low Impact Changes Already Approved

Two further versions are scheduled. CIP-003-10 carries the virtualization revisions and becomes effective July 1, 2028. CIP-003-11, approved in Order No. 918, builds on those revisions and becomes effective July 1, 2029. According to the order, CIP-003-11 adds three categories of controls for assets containing low impact BES Cyber Systems with external routable connectivity: authenticating remote users, protecting authentication information in transit, and detecting malicious communications to or between those assets. In my view,

programs that build those capabilities into their next equipment refresh will spend less than programs that retrofit them in 2029.

For executives

Low impact is where the number of assets is largest and where the requirements are changing fastest. Three versions of CIP-003 take effect between April 2026 and July 2029.

For engineers and operators

Section 3 decisions depend on knowing every routable path that leaves the asset. If you cannot draw it, you cannot show that only necessary access is permitted.

> **From the Field**
>
> Low impact controls exist because low impact systems still touch reliability.
>
> A low impact program built around the minimum is a program that hasn't read CIP-003 closely.
>
> In my view, the evidence for a low impact plan is lighter than for medium, but the program rigor expected behind it is not. Attachment 2 of CIP-003-9 lists the kinds of evidence an audit team will look for, section by section.

4 Medium Impact CIP: Reliability Significance and Oversight Focus

Medium impact is where the CIP family opens up. A medium impact rating brings in personnel and training, perimeters, system security management, incident response, recovery, configuration management, information protection, and supply chain risk management. This chapter explains why, and how the obligations vary inside the medium tier.

4.1 The Reliability Role of Medium Impact Systems

Medium impact systems support facilities whose loss would be felt beyond a single location: large generating plants, high-voltage stations, IROL-critical facilities, load-shedding schemes of 300 MW or more, and many Control Centers. Compromise of these systems can impair an operator's ability to see the system, control it, or restore it, even if no equipment fails. The criteria in CIP-002 Attachment 1, Section 2 are written around exactly those consequences.

4.2 What a Medium Impact Rating Brings In

CIP-003-9 R1.1 lists the policy topics an entity must cover for its high and medium impact BES Cyber Systems. Each points to a standard with its own requirements.

- CIP-004-7, personnel and training
- CIP-005-7, Electronic Security Perimeters, including Interactive Remote Access
- CIP-006-6, physical security of BES Cyber Systems
- CIP-007-6, system security management
- CIP-008-6, incident reporting and response planning
- CIP-009-6, recovery plans
- CIP-010-4, configuration change management and vulnerability assessments
- CIP-011-3, information protection
- declaring and responding to CIP Exceptional Circumstances

CIP-013-2, supply chain risk management, also applies to high and medium impact BES Cyber Systems.

4.3 The External Routable Connectivity Split

The medium tier is not uniform. Many requirement parts apply only to medium impact BES Cyber Systems with External Routable Connectivity, which the Glossary defines as the ability to access a BES Cyber System from a Cyber Asset outside its Electronic Security Perimeter through a bi-directional routable protocol connection.

The split shows up across the family. Under CIP-006-6, a medium impact system without External Routable Connectivity needs operational or procedural controls to restrict physical access (Part 1.1), while one with it needs at least one physical access control that limits

unescorted access to authorized individuals (Part 1.2). Under CIP-005-7, the Electronic Access Point and Interactive Remote Access parts apply to medium impact systems with External Routable Connectivity. Several CIP-004-7 parts, including training, personnel risk assessments, and access reviews, carry the same qualifier.

That makes the connectivity determination almost as consequential as the rating itself.

4.4 Control Centers and Associated Systems

Some parts reach further for medium impact systems at Control Centers. CIP-009-6 recovery plan requirements apply to medium impact BES Cyber Systems at Control Centers. CIP-005-7 Part 1.5 requires methods for detecting known or suspected malicious communications at Electronic Access Points for medium impact systems at Control Centers. Separately, CIP-012-2, effective July 1, 2026, requires plans to protect Real-time Assessment and Real-time monitoring data transmitted between Control Centers.

Associated systems carry obligations as well. A Protected Cyber Asset takes the impact rating of the highest rated BES Cyber System in the same Electronic Security Perimeter. Electronic Access Control or Monitoring Systems and Physical Access Control Systems appear in the applicability columns of most medium impact requirements.

4.5 Internal Network Security Monitoring

CIP-015-1, approved in FERC Order No. 907 and listed by NERC as effective October 1, 2028, requires internal network security monitoring within the Electronic Security Perimeters of high impact systems and medium impact systems with External Routable Connectivity. CIP-015-2, listed as effective October 1, 2029, extends the applicable systems to the associated EACMS, PACS, Protected Cyber Assets and Shared Cyber Infrastructure.

For executives

A medium impact rating is a commitment to an ongoing program across most of the CIP family, with recurring 35-day, quarterly, and 15-month cycles. Budget and staff for the cycles, not just the initial build.

For engineers and operators

External Routable Connectivity decides which parts apply. Document the determination for each medium impact system and revisit it whenever the network changes.

> **From the Field**
>
> Medium impact controls were designed for a particular operating profile. If your facility's operations or connectivity have changed since the impact classification was set, your controls may no longer match your actual risk.

5 Comparing Low and Medium Impact Requirements

This chapter lays the two tiers side by side. The intent is the same. The scope and rigor are not. Low impact requirements ask whether basic protections exist at each asset. Medium impact requirements prescribe specific controls, intervals, and evidence for each system.

5.1 Proportional Structure Within the CIP Framework

The framework has three tiers, high, medium, and low, calibrated to the consequence of compromise. The calibration is deliberate. It concentrates prescriptive controls where a compromise would do the most harm and keeps baseline controls everywhere else in scope.

5.2 Side by Side

The table summarizes the currently enforceable requirements. It is a map, not a substitute for the standards. Applicability qualifiers, especially External Routable Connectivity and Control Center location, change which medium impact parts apply.

Topic	Low impact (CIP-003-9, Attachment 1)	Medium impact
Identification	List of assets containing low impact systems (CIP-002 R1.3)	List of each medium impact BES Cyber System (CIP-002 R1.2)
Policy	Seven low impact topics, 15-month review (CIP-003 R1.2)	Nine topics, 15-month review (CIP-003 R1.1)
Awareness and training	Reinforce practices every 15 months (Section 1)	Quarterly awareness; training every 15 months where applicable (CIP-004-7)
Physical access	Need-based control of the asset or system locations (Section 2)	Physical Security Perimeters and access controls (CIP-006-6)
Electronic access	Permit only necessary routable access leaving the asset; authenticate dial-up (Section 3)	Electronic Security Perimeters, Electronic Access Points, Intermediate Systems, encryption, and multi-factor authentication for Interactive Remote Access (CIP-005-7)
Incident response	Plan tested every 36 months (Section 4)	Plan tested every 15 months; E-ISAC and NCCIC notification timelines (CIP-008-6)
Transient devices	Malicious code mitigation plan (Section 5)	Transient Cyber Asset and Removable Media plans (CIP-010-4)
Vendor remote access	Determine, disable, detect (Section 6)	Determine and disable active vendor sessions (CIP-005-7 Parts 2.4 and 2.5)

Topic	Low impact (CIP-003-9, Attachment 1)	Medium impact
Configuration and patching	No equivalent requirement	Baselines, change control, 35-day patch evaluation, vulnerability assessments (CIP-007-6, CIP-010-4)
Recovery	No equivalent requirement	Recovery plans at Control Centers (CIP-009-6)
Information protection	No equivalent requirement	BES Cyber System Information program (CIP-011-3)
Supply chain	No equivalent requirement	Supply chain risk management plans (CIP-013-2)

5.3 Reliability Consequence as the Differentiator

The table reflects consequence, not threat. The framework does not assume medium impact systems are more likely to be attacked. It assumes a successful attack on them would cost more. As the consequence rises, the standards add controls, shorten intervals, and require more specific evidence.

5.4 Consistency Without Uniformity

The CIP standards expect consistent results, not identical implementations. CIP-003 lets an entity build low impact plans by asset or group and reuse its medium impact processes. Medium impact requirements frequently allow methods "per Cyber Asset capability" or "where technically feasible." What has to be consistent is the outcome and the evidence that shows it.

5.5 Avoiding Over- or Under-Application

Applying medium impact controls to low impact assets adds cost and complexity that the standards do not require. Applying low impact controls to a system that is actually medium impact creates a compliance gap across most of the CIP family at once. Both start at the same place, the CIP-002 determination, and both are cheaper to fix before audit than after.

For executives

The comparison is a budgeting tool. Every system moved between tiers moves real obligations, cycles, and evidence with it.

For engineers and operators

When a design change could alter a rating or a connectivity determination, check the table before the change, not after.

> **From the Field**
>
> In my view, the most effective programs treat low and medium as a single risk-based architecture with proportional controls.

6 Governance and Accountability Across Low and Medium Impact Systems

Governance is where the CIP standards name names. They require a single accountable senior official, documented delegations, policies reviewed on a fixed cycle, and approval of the categorization itself. This chapter covers those obligations and how accountability should scale between the tiers.

6.1 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-003-9 R3 requires the entity to identify that person by name and document any change within 30 calendar days.

The role carries recurring duties. The CIP Senior Manager or delegate approves the CIP-002 identifications at least once every 15 calendar months under CIP-002 R2.2. The CIP Senior Manager approves the cyber security policies on the same cycle under CIP-003 R1.

6.2 Delegation

CIP-003-9 R4 lets the CIP Senior Manager delegate authority for specific actions where the CIP standards allow it. Each delegation must be documented with the delegate's name or title, the actions delegated, and the date, approved by the CIP Senior Manager, and updated within 30 days of any change. Delegations do not need to be reinstated when the delegator changes.

6.3 Scaling Accountability With Impact

For low impact assets, accountability can often sit close to the facility, with the plant or substation team responsible for the plan sections at their site. For medium impact systems, the obligations cross functions. Access authorization, patching, configuration baselines, and supply chain controls each involve different teams, and somebody above those teams has to own the result. In my view, the governance structure should be drawn to match the obligations, not the org chart.

6.4 Organizational Awareness and Role Clarity

Each group that touches a BES Cyber System should know which systems it touches and what rating they carry. For low impact, that may be the operations and engineering staff at the site. For medium impact, it usually includes operations, engineering, IT, security, and procurement.

Role clarity is not a formality. Most of the periodic requirements depend on someone remembering a cycle.

6.5 Continuity Through Organizational Change

Reorganizations, turnover, and acquisitions are where governance breaks. A CIP Senior Manager who leaves starts a 30-day clock under R3. A delegate who changes roles starts another under R4. Programs that track these as events, rather than discovering them at the next policy review, avoid a predictable class of findings.

6.6 Oversight Perspective

An audit team evaluates whether governance actually works: whether the named official exists, whether approvals happened on cycle, and whether delegations were documented before they were used. The standards do not prescribe an organizational design. They require evidence that accountability is assigned and exercised.

For executives

The CIP Senior Manager is a named, audited role. Whoever holds it should know they hold it, and should see the approvals they sign.

For engineers and operators

Governance defines your authority and your hand-offs. Know who approves changes to the systems you work on, and know who to tell when something changes.

> **From the Field**
>
> Governance escalates with consequence. Low impact governance can be lighter; medium impact cannot. The accountability hooks are different and the documentation has to reflect that.
>
> A governance program that hasn't been exercised is a governance program that doesn't exist for audit purposes. Incident response tests, every 36 months for low impact and every 15 months for medium, produce evidence that policies alone don't.

7 Personnel and Access Considerations for Low and Medium Impact Systems

People reach BES Cyber Systems through physical access, local logins, and remote sessions. Every one of those paths is a control point. This chapter compares how the two tiers handle them.

7.1 Human Interaction as a Reliability Interface

Operators, technicians, engineers, and vendors all interact with BES Cyber Systems. An unintentional action, such as a misconfiguration or a missed step in a procedure, can have the same reliability effect as a malicious one. The CIP standards address both by controlling who can reach a system, confirming that access is still needed, and removing it when it is not.

7.2 Low Impact: Need-Based Access at the Asset

CIP-004 does not apply to low impact BES Cyber Systems. Low impact personnel and access obligations come from CIP-003-9 Attachment 1:

- Section 1 requires reinforcement of cyber security practices at least once every 15 calendar months.
- Section 2 requires physical access to the asset, or to the locations of the low impact systems within it, to be controlled based on need as determined by the entity.
- Section 3 limits routable electronic access leaving the asset to what is necessary and requires authentication of dial-up.
- Section 6 requires methods to determine and disable vendor electronic remote access, and to detect known or suspected malicious communications for it.

The entity decides what "need" means. The evidence has to show that the decision was made and enforced.

7.3 Medium Impact: The CIP-004-7 Program

CIP-004-7 applies to high and medium impact BES Cyber Systems, with many parts limited to medium impact systems with External Routable Connectivity and their associated EACMS and PACS. Key obligations include:

- **Security awareness** at least once each calendar quarter (Part 1.1).
- **Training** completed at least once every 15 calendar months (Part 2.3).
- **Personnel risk assessments** completed within the last seven years for individuals with authorized electronic or unescorted physical access (Part 3.5).

- **Access verification** at least once each calendar quarter that individuals with active access have authorization records (Part 4.2), and a review at least once every 15 calendar months that accounts and privileges are correct and necessary (Part 4.3).
- **Revocation** of unescorted physical access and Interactive Remote Access within 24 hours of a termination action (Part 5.1).

7.4 Access as a Process, Not a State

Access is granted, used, reviewed, and removed. Each step needs evidence. Quarterly verification compares who is authorized against who actually has access. The 15-month review checks whether the privileges themselves are still right. Revocation timelines start at the termination action, not when someone notices.

7.5 Continuity Through Personnel Changes

Transfers and reassignments are as important as terminations. A person who moves to a role that no longer needs access should lose it. For medium impact systems, those changes typically involve HR, security, IT, and the system owner. For low impact assets, the site team may handle it directly, but the need-based decision still has to be current.

For executives

Personnel and access controls depend on HR and contractor processes the compliance team does not own. Make sure termination and transfer notices reach the people who remove access, on the clock the standard sets.

For engineers and operators

Your access is part of the compliance record. Shared accounts, borrowed badges, and undocumented vendor sessions are evidence problems as well as security problems.

> **From the Field**
>
> In my view, personnel and access controls tell you more about a CIP program's actual security posture than any other part of it. CIP-004 sat among the three most frequently reported CIP noncompliance areas in NERC's 2025 annual report.
>
> In my view, a revoked credential that is still active is one of the easiest findings to prevent. CIP-004-7 Part 5.1 sets the clock at 24 hours for unescorted physical access and Interactive Remote Access.

8 System Security Concepts for Low and Medium Impact Systems

Technical controls are where the difference between the tiers is most visible. Low impact assets need a defensible boundary and protection against malicious code arriving on transient devices. Medium impact systems need perimeters, hardened configurations, patching, logging, and configuration management on fixed cycles.

8.1 Technical Protection as Reliability Support

The technical controls in CIP exist so that systems behave predictably under normal and abnormal conditions. A control that blocks an unneeded port, catches an unauthorized change, or flags a suspicious login protects the operator's ability to see and control the system.

8.2 Boundaries: The Asset Edge Versus the Electronic Security Perimeter

The two tiers draw boundaries differently.

For low impact, the boundary is the asset. CIP-003-9 Section 3 controls routable communications that cross into or out of the asset containing low impact BES Cyber Systems. It excludes communications used for time-sensitive protection or control functions between intelligent electronic devices, such as IEC TR-61850-90-5 R-GOOSE. There is no Electronic Security Perimeter requirement for low impact systems.

For medium impact, the boundary is the Electronic Security Perimeter, defined as the logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol. CIP-005-7 Part 1.1 requires every applicable Cyber Asset connected by a routable protocol to reside within a defined ESP. For systems with External Routable Connectivity, all such connectivity must pass through an identified Electronic Access Point (Part 1.2), which must require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default (Part 1.3).

8.3 Remote Access

Interactive Remote Access to medium impact systems with External Routable Connectivity must pass through an Intermediate System so the initiating device does not directly access the applicable Cyber Asset, must be encrypted to the Intermediate System, and must use multi-factor authentication (CIP-005-7 Parts 2.1 through 2.3). Entities must also be able to determine and disable active vendor remote access sessions (Parts 2.4 and 2.5). Low impact vendor remote access falls under CIP-003-9 Section 6.

8.4 Hardening, Patching, and Malicious Code

For medium impact systems with External Routable Connectivity, CIP-007-6 requires enabling only needed logical network ports and services where technically feasible (Part 1.1). For all medium impact systems it requires evaluating security patches at least once every 35 calendar days (Part 2.2) and, within 35 days of each evaluation, applying the patch or creating or revising a dated mitigation plan (Part 2.3). It also requires methods to deter, detect, or prevent malicious code (Part 3.1). For low impact, the malicious code obligation is specific to Transient Cyber Assets and Removable Media under CIP-003-9 Section 5.

8.5 Change, Configuration, and Stability

Unplanned change is a reliability risk. CIP-010-4 requires medium impact systems to have a documented baseline configuration (Part 1.1), authorized and documented changes (Part 1.2), baseline updates within 30 calendar days of a change that deviates from it (Part 1.3), and a paper or active vulnerability assessment at least once every 15 calendar months (Part 3.1). Low impact systems have no configuration management requirement, although an entity's own change practices are often what keep its Section 3 controls accurate.

8.6 Technical Controls in Organizational Context

A control that operators work around does not protect anything. Technical controls have to fit the way the system is actually operated and maintained, and the people who run them have to understand why they exist. That is why CIP pairs technical requirements with training, change control, and governance.

For executives

Architecture choices set compliance cost for years. A network that minimizes routable paths into medium impact systems reduces the number of controls that must be built, evidenced, and reviewed.

For engineers and operators

Every firewall rule and open port on a medium impact Electronic Access Point needs a documented reason. Every change to a baseline needs a record within 30 days.

> **From the Field**
>
> A firewall rule that's never been reviewed internally is a firewall rule that may not do what its name suggests. CIP-005 requires a documented reason for every permitted access at a medium impact Electronic Access Point, and CIP-010 requires the baseline to keep up with change.
>
> System hardening that wasn't validated against actual operating conditions is documentation, not protection.

9 Monitoring, Detection, Response, and Recovery Across Impact Levels

Prevention fails eventually. The question then is whether the entity notices, responds in a coordinated way, reports what it must, and restores the system. The CIP standards scale each of those capabilities with impact.

9.1 Cyber Events as Reliability Conditions

A cyber event matters to the CIP standards because of what it can do to the reliable operation of the system. The NERC Glossary defines a Cyber Security Incident as 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 EACMS, or that disrupts or attempts to disrupt the operation of a BES Cyber System. A Reportable Cyber Security Incident is one that compromised or disrupted a BES Cyber System performing a reliability task, or the ESP or EACMS of a high or medium impact system.

9.2 Monitoring and Detection

For low impact assets, detection obligations are narrow today. CIP-003-9 Section 6.3 requires methods for detecting known or suspected malicious communications for vendor electronic remote access. CIP-003-11, effective July 1, 2029, will add detection of malicious communications to or between assets containing low impact systems with external routable connectivity.

For medium impact systems, CIP-007-6 Part 4.1 requires logging of events for identification and after-the-fact investigation of Cyber Security Incidents, including detected successful login attempts and detected failed access attempts. Part 4.3 requires retaining those logs for at least 90 consecutive calendar days where technically feasible for the applicable systems, which include medium impact systems at Control Centers. At Control Centers, CIP-005-7 Part 1.5 adds detection of malicious communications at Electronic Access Points. CIP-015-1 and CIP-015-2 will add internal network security monitoring in 2028 and 2029.

9.3 Response and Reporting

Both tiers require a Cyber Security Incident response plan. The low impact plan under CIP-003-9 Section 4 must cover reportability, notification to the E-ISAC, roles, incident handling, testing at least every 36 calendar months, and updates, if needed, within 180 days of a test or actual incident.

For medium impact systems, CIP-008-6 requires testing at least once every 15 calendar months (Part 2.1). It also sets notification timelines to the E-ISAC and to the National Cybersecurity and Communications Integration Center: within one hour after determining a Reportable Cyber

Security Incident, and by the end of the next calendar day after determining that a Cyber Security Incident was an attempt to compromise an applicable system (Part 4.2). Updates follow within 7 calendar days of new or changed information (Part 4.3).

9.4 Recovery and Resilience

CIP-009-6 requires recovery plans for high impact systems and for medium impact systems at Control Centers, with testing on a 15-month cycle. Low impact assets and medium impact systems outside Control Centers have no CIP recovery plan requirement. That does not mean recovery is unimportant there. It means the obligation comes from the entity's operating practice rather than the standard.

9.5 Learning and Continuous Awareness

Incident tests and real events both feed back into the plan. The low impact plan must be updated, if needed, within 180 calendar days after a test or actual Reportable Cyber Security Incident, and medium impact plans carry their own review, update, and communication obligations under CIP-008-6 Requirement R3. Programs that treat each test as a chance to fix something, rather than a box to check, improve faster.

For executives

Notification timelines are measured in hours. Decide in advance who has authority to declare an incident reportable and who makes the call to the E-ISAC.

For engineers and operators

The logs you keep and the anomalies you notice are what turn a suspicion into a determination. Know what your systems log, how long they keep it, and who reviews it.

10 Compliance Monitoring and Enforcement for Low and Medium Impact CIP

Low and medium impact requirements are mandatory and enforceable. They are monitored and enforced through the same program as every other Reliability Standard. The impact rating changes what is required, not whether it is enforced.

10.1 Low and Medium Impact Within the Mandatory Framework

Section 215 of the Federal Power Act, 16 U.S.C. 824o, provides for mandatory and enforceable Reliability Standards developed by the Electric Reliability Organization and approved by FERC. The NERC Glossary defines a Reliability Standard as a requirement approved by FERC under Section 215, and expressly includes cybersecurity protection of existing Bulk-Power System facilities. Every CIP standard discussed in this reference, at every impact level, sits inside that framework.

10.2 How Compliance Is Monitored

The Compliance Monitoring and Enforcement Program in Appendix 4C of the NERC Rules of Procedure lists the monitoring processes: Compliance Audits, Self-Certifications, Spot Checks, Compliance Investigations, Self-Reports, Self-Logging, Periodic Data Submittals, and Complaints. The Compliance Enforcement Authority determines the type and frequency of monitoring based on the registered entity's specific risks to the reliability of the Bulk Power System.

For Compliance Audits, the Compliance Enforcement Authority notifies the entity at least 90 days before a scheduled audit and identifies the standards to be evaluated. Audit scope is tailored using risk-based inputs, including Inherent Risk Assessments and internal controls.

10.3 Low Impact Is Audited

The ERO Enterprise CIP Evidence Request Tool flags each asset that contains a low impact BES Cyber System on its BES Assets tab. A separate Low Cyber Asset tab is optional, for entities that keep a list of their low impact systems. An entity with only low impact assets should expect its asset list, its CIP-003 plan, and the evidence behind each plan section to be examined.

10.4 Risk-Informed Enforcement

When monitoring finds a potential noncompliance, the CMEP routes it through a preliminary screen and then into enforcement, and the entity must mitigate it. The ERO Enterprise uses

streamlined dispositions for lower-risk issues. NERC's 2025 annual report states that the ERO Enterprise processed approximately 83% of filed or submitted noncompliance as Compliance Exceptions and 14% as Find, Fix, Track in 2025, and that registered entities self-identified approximately 85% of reported noncompliance.

10.5 Where CIP Noncompliance Clusters

The same report lists the ten most frequently reported CIP noncompliance areas in 2025, in order: CIP-010, CIP-007, CIP-004, CIP-003, CIP-006, CIP-011, CIP-002, CIP-005, CIP-009, and CIP-013. It identifies lack of or deficient policies and procedures as the leading root cause for the top three. CIP-003, the home of the low impact plan, ranks fourth.

10.6 Compliance and Risk Reduction

An audit tests whether the required controls exist and operate as documented. It does not certify that a system is secure. The standards set a floor. Reliability depends on how well the entity runs the system above that floor.

For executives

Self-identification is the norm, not the exception. A program that finds and reports its own issues is in a far better position than one that waits for an audit team to find them.

For engineers and operators

Evidence is produced every day the program runs. Logs, tickets, approvals, and review records created in the normal course of work are what an audit team will sample.

> **From the Field**
>
> In my view, knowing where CIP noncompliance clusters is most of the preparation.
>
> In my view, CIP audits differ from non-CIP audits in density more than in kind. The evidence requests are larger, the samples are deeper, and one scoping error can touch several requirements at once.
>
> A CIP self-report deserves the same care as the evidence behind it. Describe the scope precisely, show the mitigation, and expect the Region to ask whether the same gap exists at other assets.

11 Common Misunderstandings About Low and Medium Impact CIP

Most of the errors in this chapter are not about a specific requirement. They are about what the ratings mean. Each one leads to a predictable kind of gap.

11.1 "Low Impact" Does Not Mean Low Importance

Low impact describes the consequence of compromising one system, measured against the Attachment 1 criteria. It says nothing about whether the system matters to the facility or to the people who run it. Low impact systems still carry an enforceable plan, and FERC has stated its concern about coordinated attacks across many of them.

11.2 Low Impact Does Not Mean No Inventory

CIP-002 R1.3 does not require a discrete list of low impact BES Cyber Systems. It does require a list of the assets that contain them. And CIP-003 Section 3 cannot be met without knowing which communications leave each asset. In my view, an entity that cannot describe what is inside a low impact asset will struggle to show that only necessary access is permitted.

11.3 Medium Impact Is Not a Stepping Stone to High Impact

Medium impact is not a waiting room. High impact applies only to the Control Centers described in Attachment 1, Section 1. A substation or generating plant's own BES Cyber Systems will never be rated high, no matter how large it grows; only a qualifying Control Center can be. Its systems can move between low and medium as criteria are met or no longer met.

11.4 Impact Classification Is Not a Threat Assessment

The rating measures consequence, not likelihood. A low impact system may face the same threats as a medium impact one. The difference is what happens to the Bulk Electric System if an attack succeeds.

11.5 Applicability Is Not Organization-Wide

Ratings attach to BES Cyber Systems at in-scope assets. They do not cover the corporate network by default, and one asset's rating does not carry to another. Over-scoping adds cost. Under-scoping adds violations.

11.6 Uniform Controls Are Not Required

Low and medium impact systems do not have to be protected in the same way as high impact systems, or in the same way as each other. Section 5.4 explains the flexibility CIP-003 allows. What the standards require is that each applicable requirement is met and evidenced.

11.7 Compliance Does Not Replace Judgment

Meeting the requirements manages baseline risk. It does not replace engineering judgment about how the system behaves, what it connects to, and what would happen if it failed. The standards define the minimum. The people running the system define everything above it.

11.8 Oversight Is Not Adversarial

The CMEP is built around risk. Most noncompliance is self-identified and most is resolved as a Compliance Exception, according to NERC's 2025 annual report. Oversight is about accountability, consistency, and visibility, and entities that engage with it openly tend to fare better.

11.9 Responsibility Is Broader Than the Compliance Team

Operations, engineering, IT, procurement, and HR all make decisions that change CIP scope or affect a control. A new remote access path, a vendor contract, or a reorganization can each create an obligation the compliance team never saw coming.

> **From the Field**
>
> "Low impact means light obligations" is a misunderstanding with a cost. CIP-003, home of the low impact plan, ranked fourth among reported CIP noncompliance in 2025. Light is not the same as absent.

12 Executive and Engineering Takeaways

This chapter pulls the reference together for two audiences: the leaders who own the program and the engineers and operators who run the systems.

12.1 Proportionality Is the Foundation

The CIP standards scale controls to the consequence of compromise. Three ratings, set by CIP-002 Attachment 1, decide which requirements apply. Every downstream obligation depends on getting that determination right and keeping it current every 15 months.

12.2 Low Impact Does Not Mean Minimal Responsibility

Low impact systems carry a policy, a named CIP Senior Manager, and a six-section plan under CIP-003-9. The requirements are less prescriptive than medium impact, but they are enforced, audited, and expanding.

12.3 Medium Impact Reflects Broader Operational Influence

Medium impact systems support facilities whose loss would be felt beyond one site. The rating brings in most of the CIP family, with External Routable Connectivity and Control Center location deciding which parts apply.

12.4 Governance Shapes Reliability Outcomes

Named accountability, documented delegations, and approvals on cycle are requirements, not preferences. Executive decisions about staffing, architecture, and vendors set the conditions the program operates under.

12.5 Engineering Judgment Remains Central

The standards say what must be achieved and often how it must be evidenced. They do not design the network or operate the plant. That judgment belongs to the people who know the system.

12.6 Compliance Supports but Does Not Define Reliability

Compliance demonstrates that required controls exist and work. Reliability depends on the whole system, including everything the standards do not reach.

12.7 The Calendar Ahead

The requirements in this reference will change on known dates. Plan for them now.

Effective date	Change
April 1, 2026	CIP-003-9 in effect, adding low impact vendor electronic remote access controls
July 1, 2026	CIP-012-2 in effect for communications between Control Centers
July 1, 2028	Virtualization revisions across the CIP family, including CIP-003-10, CIP-005-8, CIP-007-7.1, and CIP-010-5, plus CIP-002-8 (which supersedes CIP-002-7) and the revised Control Center definition
October 1, 2028	CIP-015-1 internal network security monitoring
July 1, 2029	CIP-003-11 low impact authentication, protection of authentication information in transit, and malicious communication detection
October 1, 2029	CIP-015-2, extending internal network security monitoring to associated EACMS, PACS, and Protected Cyber Assets

For executives

Use the calendar to set budgets. The 2028 and 2029 changes affect architecture and tooling, and both take lead time.

For engineers and operators

Use the calendar to set design standards. Equipment bought in 2027 will still be in service when CIP-003-11 takes effect.

Glossary

Definitions marked as NERC Glossary terms are quoted or closely paraphrased from the Glossary of Terms Used in NERC Reliability Standards as currently enforceable. Several of these definitions change on July 1, 2028 under the virtualization standards. Check the Glossary for the version in force.

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 is not considered. Each BES Cyber Asset is included in one or more BES Cyber Systems. (NERC Glossary)
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. (NERC Glossary)
BES Cyber System Information	Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. (NERC Glossary)
Bulk Electric System (BES)	Unless modified by the inclusions and exclusions in the definition, 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. (NERC Glossary)
CIP Exceptional Circumstance	A situation that involves or threatens to involve conditions that impact safety or BES reliability, such as a risk of injury or death, a natural disaster, civil unrest, an imminent or existing 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. (NERC Glossary)
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. (NERC Glossary)

Term	Meaning in this paper
Control Center	One or more facilities hosting operating personnel that monitor and control the BES in real-time to perform the reliability tasks, including their associated data centers, of a Reliability Coordinator, a Balancing Authority, a Transmission Operator for transmission Facilities at two or more locations, or a Generator Operator for generation Facilities at two or more locations. The revised definition effective July 1, 2028 adds certain Transmission Owner facilities with SCADA control at two or more locations. (NERC Glossary)
Critical Infrastructure Protection (CIP) standards	The family of NERC Reliability Standards, CIP-002 through CIP-015, that sets cyber and physical security requirements for the Bulk Electric System.
Cyber Assets	Programmable electronic devices, including the hardware, software, and data in those devices. (NERC Glossary)
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 EACMS; or disrupts or attempts to disrupt the operation of a BES Cyber System. (NERC Glossary)
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, including Intermediate Systems. (NERC Glossary)
Electronic Security Perimeter (ESP)	The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol. (NERC Glossary)
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. (NERC Glossary)
Impact rating	The high, medium, or low categorization of a BES Cyber System under CIP-002 Attachment 1, based on the adverse impact its loss, compromise, or misuse could have on the reliable operation of the BES.
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 inside any of the entity's Electronic Security Perimeters or at a defined Electronic Access Point. It does not include system-to-system process communications. (NERC Glossary)
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. (NERC Glossary)
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 ESP. Their impact rating equals that of the highest rated BES Cyber System in the same ESP. (NERC Glossary)
Registered Entity	An owner, operator, or user of the Bulk Power System, or the entity registered as its designee for the purpose of compliance, that is included in the NERC Compliance Registry. (NERC Rules of Procedure, Appendix 2)

Term	Meaning in this paper
Reliability Standard	A requirement, approved by FERC under Section 215 of the Federal Power Act, or approved or recognized by an applicable governmental authority in other jurisdictions, to provide for Reliable Operation of the Bulk-Power System, including cybersecurity protection. (NERC Glossary)
Removable Media	Storage media that are not Cyber Assets, are capable of transferring executable code, can be used to store, copy, move, or access data, and are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP containing high or medium impact BES Cyber Systems, or an associated Protected Cyber Asset. (NERC Glossary)
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, or an Electronic Security Perimeter or EACMS of a high or medium impact BES Cyber System. (NERC Glossary)
Transient Cyber Asset	A Cyber Asset that is capable of transmitting or transferring executable code, is not included in a BES Cyber System, is not a Protected Cyber Asset associated with high or medium impact BES Cyber Systems, and is directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a Protected Cyber Asset. (NERC Glossary)

How Energy Compliance Can Help

CIP programs succeed or fail on the categorization and the evidence behind it. Energy Compliance services related to Critical Infrastructure Protection include, but are not limited to:

- 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
- CIP governance and program assessments
- Integration of cybersecurity oversight with broader reliability programs
- Audit and enforcement support for CIP findings (non-advocacy)
- CIP framework reviews, gap analyses, and improvement plans
- Training focused on CIP framework, requirements, and audit expectations
- Executive and board-level CIP awareness briefings

Around that core, EC provides audit defense with Notice of Penalty response and settlement posture, RSAW production, and data request strategy; registration and applicability analysis for new generator registrants, including Category 2 IBRs; NERC compliance program support, interpretation, and audit preparation; senior advisory on complex reliability questions; and industry engagement in standards development and working-group participation. Services are tailored to the functional role, system impact, and regulatory posture of each organization.

WattOps Compliance is EC's NERC compliance evidence platform (wattopscompliance.com). It keeps the evidence behind your non-CIP obligations organized while your team works the 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 solar, wind, and storage operators, any routable operations-data path that leaves an asset containing low impact BES Cyber Systems belongs in that asset's Section 3 electronic access determination.

Start with your CIP-002 determination. If you cannot explain every rating in writing, call us.

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.

Our CIP-focused services are listed in How Energy Compliance Can Help.

Learn more at energycomplianceinc.com.

Sources and Authorities

- North American Electric Reliability Corporation (NERC), Reliability Standard CIP-002-5.1a, Cyber Security: BES Cyber System Categorization, including Attachment 1, Impact Rating Criteria (effective December 27, 2016). 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, including Attachment 1 and Attachment 2 (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/pa/Stand/Reliability%20Standards/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 Standards CIP-015-1 and CIP-015-2, Cyber Security: Internal Network Security Monitoring (subject to future enforcement October 1, 2028 and

October 1, 2029). https://www.nerc.com/globalassets/standards/reliability-standards/cip/cip-015-1.pdf ; https://www.nerc.com/globalassets/standards/reliability-standards/cip/cip-015-2.pdf
- NERC, Reliability Standards: CIP standards listing with status and effective dates. https://www.nerc.com/standards/reliability-standards/cip
- NERC, Glossary of Terms Used in NERC Reliability Standards. https://www.nerc.com/glossary-of-terms
- NERC, Rules of Procedure, Appendix 2, Definitions Used in the Rules of Procedure. https://www.nerc.com/globalassets/who-we-are/rules-of-procedure/Appendix-2.pdf
- 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, ORCP and CMEP Annual Report (February 11, 2026). https://www.nerc.com/globalassets/programs/enforcement/cmep-and-vegetation-reports/2025-orcp-and-cmep-annual-report.pdf
- NERC, 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 & 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
- Federal Energy Regulatory Commission (FERC), Order No. 918, Critical Infrastructure Protection Reliability Standard CIP-003-11, Cyber Security: Security Management Controls, Docket No. RM25-8-000 (March 19, 2026). https://www.govinfo.gov/content/pkg/FR-2026-03-24/pdf/2026-05711.pdf
- FERC, North American Electric Reliability Corporation; Order Approving Reliability Standard CIP-002-8, Docket No. RD25-8-000 (March 19, 2026). https://www.govinfo.gov/content/pkg/FR-2026-03-24/pdf/2026-05715.pdf
- FERC, 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
- Federal Power Act Section 215, Electric Reliability, 16 U.S.C. 824o. https://www.law.cornell.edu/uscode/text/16/824o

© Energy Compliance, Inc. · EC-WP-201 · October 2026