CYBERSECURITY · CIP SERIES · EC-WP-202

CIP Medium Impact Deep Dive

Medium Impact CIP scope, risk logic, and reliability control structures.

Medium impact is where CIP stops being a plan and becomes a full control architecture. This reference walks the medium impact obligations standard by standard, from the CIP-002 criteria through governance, perimeters, system security, configuration, information protection, and incident response and recovery. It covers the requirements in force in October 2026, what NERC's latest enforcement data says about where programs fail, 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.

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

Medium impact BES Cyber Systems sit at the generating plants, transmission stations, and Control Centers whose compromise could hurt the Bulk Electric System, but which CIP-002 does not reserve for the high impact tier. The controls for this tier are calibrated to protect those systems without breaking the high-availability, low-downtime operating environments they live in. Get the calibration wrong in either direction and the program produces the wrong outcome: over-engineered, under-protected, or both.

This reference walks the medium impact obligations in the order a program experiences them. It starts with the CIP-002 categorization that creates the obligation, moves through governance, perimeters, personnel and physical access, system security, configuration, information protection, and incident response and recovery, and ends with how the ERO Enterprise audits the tier and what changes in 2028 and 2029. Each requirement cited is to the version in force in October 2026.

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

- The medium impact rating is a threshold determination, and every downstream obligation inherits its accuracy.
- CIP-003 is where CIP becomes a managed program rather than a set of technical controls. Nine policy topics, one named CIP Senior Manager, and a 15-month review cycle hold the rest together.
- CIP-005 defines the Electronic Security Perimeter. In my view the dangerous CIP-005 problem is an undocumented crossing, not a failed control.
- Physical security is not secondary to electronic security. A bypass at the physical layer makes the electronic controls irrelevant, and stale access is a CIP-004 problem as much as a CIP-006 one.
- CIP-007 and CIP-010 are where most of the operational compliance effort lives. NERC's 2025 annual report names CIP-010, CIP-007, and CIP-004 as the most frequently reported CIP noncompliance, with deficient policies and procedures as the leading root cause.
- CIP-008 and CIP-009 plan for the incident that gets through: tested response plans, a one-hour reporting clock, and recovery plans.
- The requirements are moving. Virtualization revisions across the CIP family and a revised CIP-002 take effect July 1, 2028. Internal network security monitoring under CIP-015-1 reaches medium impact systems with External Routable Connectivity on October 1, 2028.

1 CIP-002 and the Logic of Medium Impact Classification

Every obligation in this reference flows from one determination. CIP-002 decides whether a BES Cyber System is high, medium, or low impact, and that rating decides which requirements apply and how deep they run. Medium impact is a threshold, and the threshold is set by the consequence of compromise.

1.1 The Design Compromise Behind the Tier

Medium impact controls answer two competing needs. The first is adequate protection against cyber and physical threats, so that the control systems running generation and transmission keep operating without disruption. The second is the operating reality of those systems: they are expected to be available all the time, with very little tolerance for downtime. The control set has to work inside that constraint.

That means the reliability test for a medium impact control is whether it preserves continuous control and system integrity. Whether it matches the security practice you would apply to an enterprise IT network is a different question, and not the one the standards ask.

1.2 Classification Comes First

CIP-002-5.1a, in force since December 27, 2016, requires each Responsible Entity to implement a process that considers 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, Cranking Paths, and initial switching requirements; Special Protection Systems; and, for Distribution Providers, certain Protection Systems. Requirement R1, Part 1.2 then requires the entity to identify each medium impact BES Cyber System at each asset according to Attachment 1, Section 2. R1 carries a High Violation Risk Factor.

The building blocks come from the NERC Glossary. A Cyber Asset is a programmable electronic device, including its hardware, software, and data. A BES Cyber Asset is a Cyber Asset that, if rendered unavailable, degraded, or misused, would adversely impact the reliable operation of the Bulk Electric System within 15 minutes of its required operation, misoperation, or non-operation. A BES Cyber System is one or more BES Cyber Assets logically grouped to perform one or more reliability tasks.

In practice the work runs in a sequence. Identify the in-scope assets. Identify the Cyber Assets at each asset that perform or support reliability tasks. Group them into BES Cyber Systems. Apply the Attachment 1 criteria to each system. A mistake at any step carries forward into every requirement that follows.

1.3 The Medium Impact Criteria

Section 2 of Attachment 1 applies to each BES Cyber System, not already rated high impact under Section 1, that is associated with any of thirteen criteria. The table below paraphrases them; the standard's exact wording controls.

Criterion	What it reaches
2.1	Generation at a single plant location with an aggregate highest rated net Real Power capability, over the preceding 12 calendar months, of 1,500 MW or more in a single Interconnection (shared systems only)
2.2	Reactive resources at a single location, excluding generation Facilities, with an aggregate maximum nameplate of 1,000 MVAR or more (shared systems only)
2.3	Generation Facilities the 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	Transmission Facilities at 200 to 499 kV at a station connected at 200 kV or higher to three or more other stations, with an aggregate weighted value exceeding 3,000
2.6	Generation or Transmission Facilities identified as critical to the derivation of IROLs and their associated contingencies
2.7	Transmission Facilities essential to meeting Nuclear Plant Interface Requirements
2.8	Transmission Facilities, including generation interconnection Facilities, whose loss would cause the loss of generation identified under 2.1 or 2.3
2.9	SPS, RAS, or automated switching Systems whose failure would cause IROL violations 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, not already high
2.12	Transmission Operator Control Centers not already high
2.13	Balancing Authority Control Centers for 1,500 MW or more in a single Interconnection, not already high

The criteria are objective by design. Capacity, voltage, connection count, and designation by a planner replace judgment about how important a facility feels. For criteria 2.1 and 2.2 the test is narrower than it first reads: only shared BES Cyber Systems that could, within 15 minutes, adversely affect a combination of units or resources reaching the threshold meet the criterion.

1.4 Why a Middle Tier at All

The middle tier was a policy choice. It applies more controls than low impact because the consequence of compromise is higher, and fewer than high impact because these facilities are

not the Reliability Coordinator, Balancing Authority, and large operator Control Centers that Section 1 reserves for the top tier. It also reflects a practical point. Not every operational technology environment can carry the same control set, and a single uniform regime would either over-burden field assets or under-protect Control Centers.

1.5 Evidence Behind the Determination

A medium impact label by itself is not evidence. Measure M1 asks for dated lists of the identifications R1 requires. A defensible program keeps more than the list: the asset inventory, the functional analysis of each Cyber Asset, and the mapping of each BES Cyber System to the specific criterion that rates it. When an auditor asks why a system is medium and not low, the answer should be a document, not a recollection.

1.6 Keeping the Determination Current

Stations evolve. Capacity changes, lines are added, Control Centers take on new functions. CIP-002-5.1a R2 requires the entity to review the R1 identifications, and update them where there are changes, at least once every 15 calendar months, and to have its CIP Senior Manager or delegate approve the identifications on the same cycle. Both apply even if the entity has no identified items. The categorization must reflect the system as it is configured now, not as it was when the program was first built.

End-of-Chapter Summary

CIP-002 defines the enforceable process for identifying and categorizing BES Cyber Systems. Attachment 1, Section 2 sets thirteen objective criteria for medium impact, and the rating then determines the depth of every control that follows. The determination must be documented, traceable to a specific criterion, and reviewed and approved at least once every 15 calendar months.

> **From the Field**
>
> CIP-002 is the gate. Everything else in CIP runs through it. Get the classification right and the rest of the program is calibrated. Get it wrong and the program is built on the wrong scope. The classification logic isn't arbitrary. It traces the consequence of compromise to a specific impact rating. Reading the rationale, not just the threshold, is what makes the classification defensible.

2 CIP-003 and Governance Controls for Medium Impact Systems

Once CIP-002 rates a system medium impact, CIP-003 supplies the management framework the technical standards operate inside. The version in force is CIP-003-9, effective April 1, 2026.

2.1 The Nine Policy Topics

CIP-003-9 R1 requires the Responsible Entity to review, and obtain CIP Senior Manager approval for, one or more documented cyber security policies at least once every 15 calendar months. For high and medium impact BES Cyber Systems, Part 1.1 requires the policies to collectively address nine topics:

1. Personnel and training (CIP-004)
2. Electronic Security Perimeters, including Interactive Remote Access (CIP-005)
3. Physical security of BES Cyber Systems (CIP-006)
4. System security management (CIP-007)
5. Incident reporting and response planning (CIP-008)
6. Recovery plans for BES Cyber Systems (CIP-009)
7. Configuration change management and vulnerability assessments (CIP-010)
8. Information protection (CIP-011)
9. Declaring and responding to CIP Exceptional Circumstances

The policy is not the procedure. R1 asks for policies that address each topic; the standards they point to carry the operational requirements. Measure M1 names the evidence: policy documents, revision history or records of review, and documented CIP Senior Manager approval for each policy within the 15-month window. R1 carries a Medium Violation Risk Factor.

2.2 The CIP Senior Manager and Delegation

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

R4 governs delegation. Where the CIP standards allow it, the CIP Senior Manager may delegate authority for specific actions. Each delegation must be documented with the delegate's name or title, the specific actions delegated, and the date, approved by the CIP Senior Manager, and updated within 30 days of any change. A delegation record that has not kept up with reorganizations is a common place for a governance program to drift without anyone noticing.

2.3 Governance as Accountability

In a medium impact environment, the line between operations and cybersecurity blurs. Plant staff touch control systems every shift. Vendors support them remotely. Engineering changes settings that matter to the perimeter. Governance answers the question of who is responsible for each piece, and it does so before the incident, not during it. Policy approval authority, named roles, and documented procedures make that responsibility visible to the people who hold it and to the auditor who will ask.

2.4 Supply Chain Belongs to CIP-013

Supply chain risk is a governance question, but it is not a CIP-003 requirement. CIP-013-2, effective October 1, 2022, requires one or more documented supply chain cyber security risk management plans for high and medium impact BES Cyber Systems and their associated EACMS and PACS. The plan must include processes for identifying and assessing cyber security risk from vendor products and services during procurement planning, and processes used in procurement that address vendor notification of vendor-identified incidents, coordination of responses to those incidents, vendor notice when access should no longer be granted, disclosure of known vulnerabilities, verification of software integrity and authenticity, and coordination of controls for vendor-initiated remote access. R2 requires the entity to implement the plan. R3 requires review and CIP Senior Manager or delegate approval at least once every 15 calendar months.

2.5 Governance That Respects Operations

The standards do not prescribe a technology or an organizational structure. Control Centers, substations, and generating plants run around the clock, and a governance process that stalls operations to satisfy paperwork has missed the point. What the standards require is that processes are defined, approved, implemented, and reviewed on cycle. How an entity organizes itself to meet that is its own decision, and the evidence should show the decision was made deliberately.

End-of-Chapter Summary

CIP-003-9 requires documented cyber security policies covering nine topics for high and medium impact systems, reviewed and approved by a named CIP Senior Manager at least once every 15 calendar months, with documented delegations. Supply chain risk management for the same systems sits in CIP-013-2. Together they set the accountability layer the technical controls depend on.

> **From the Field**
>
> Governance is what the standard expects from leadership. Procedure is what the standard expects from operations. CIP-003 holds both ends accountable. A CIP Senior Manager isn't a title; it's a named role with named responsibility, and CIP-003 expects that role to be filled by someone who knows they hold it. Policies that haven't been reviewed in fifteen months are policies that haven't been reviewed. CIP-003 sets the cadence; the program has to operate it.

3 CIP-005 and the Electronic Security Perimeter for Medium Impact Systems

CIP-005 governs the Electronic Security Perimeter and remote access. The version in force is CIP-005-7, effective October 1, 2022. For medium impact, it defines the logical boundary where access control, authentication, and monitoring must happen.

3.1 The Perimeter as a Defined Construct

The NERC Glossary defines the Electronic Security Perimeter as the logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol. An Electronic Access Point is a Cyber Asset interface on that perimeter that allows routable communication between Cyber Assets inside and outside it. External Routable Connectivity is the ability to reach a BES Cyber System from outside its perimeter over a bi-directional routable protocol connection.

That last definition does a great deal of work. Across CIP-005, CIP-006, CIP-007, and CIP-004, many medium impact requirements apply only to medium impact systems with External Routable Connectivity. Whether a system has it is a scoping decision with consequences across the program.

3.2 What R1 Requires

CIP-005-7 R1 requires documented processes that collectively include five parts:

- **Part 1.1.** All applicable Cyber Assets connected to a network via a routable protocol reside within a defined ESP. This applies to medium impact BES Cyber Systems and their associated Protected Cyber Assets.
- **Part 1.2.** All External Routable Connectivity passes through an identified Electronic Access Point.
- **Part 1.3.** Electronic Access Points require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.
- **Part 1.4.** Where technically feasible, authentication is performed when establishing Dial-up Connectivity.
- **Part 1.5.** Electronic Access Points for medium impact BES Cyber Systems at Control Centers have one or more methods for detecting known or suspected malicious communications, inbound and outbound.

The standard specifies outcomes, not technology. The measures name the evidence: a list of ESPs with their Cyber Assets, network diagrams showing every external routable

communication path and the identified EAPs, and rule sets showing that each permitted access has a documented reason.

3.3 Interactive Remote Access

Vendor support, engineering access, and operational troubleshooting routinely require someone outside the perimeter to work on a medium impact system. The Glossary defines Interactive Remote Access as user-initiated access by a person using a remote access client or other remote access technology over a routable protocol, from a Cyber Asset that is not an Intermediate System and not inside any of the entity's ESPs or at a defined EAP. It does not include system-to-system process communications.

For medium impact BES Cyber Systems with External Routable Connectivity, R2 requires, where technically feasible:

- **Part 2.1.** An Intermediate System, so the initiating Cyber Asset never directly accesses an applicable Cyber Asset.
- **Part 2.2.** Encryption for all Interactive Remote Access sessions, terminating at the Intermediate System.
- **Part 2.3.** Multi-factor authentication for all Interactive Remote Access sessions.
- **Part 2.4.** One or more methods for determining active vendor remote access sessions, including Interactive Remote Access and system-to-system remote access.
- **Part 2.5.** One or more methods to disable active vendor remote access.

R3 extends vendor remote access controls to the EACMS and PACS associated with medium impact systems with External Routable Connectivity. The entity must be able to determine authenticated vendor-initiated remote connections and to terminate them and control the ability to reconnect.

3.4 The Perimeter in the Layered Architecture

CIP-003 sets governance. CIP-007 manages the systems inside the boundary. CIP-005 is the boundary between them and the outside world, and a weakness there undercuts everything downstream. An improperly configured access point can defeat sound controls on every system behind it.

Medium impact environments make perimeter design harder. Legacy equipment, vendor restrictions on segmentation, and plant networks that grew over decades rarely match a clean reference architecture. The standard does not demand one. It demands that every applicable routable connection sits inside a defined perimeter and that every crossing is identified and controlled.

3.5 Diagrams That Match the Network

From an operational view, a network diagram shows how the BES Cyber System elements connect. From a compliance view, it is the basis for the perimeter: the auditor will compare the diagram, the rule sets, and the actual configuration. The diagram is only as good as its last update, and a perimeter that changed without the diagram changing is a perimeter the program no longer understands.

End-of-Chapter Summary

CIP-005-7 requires that medium impact BES Cyber Systems sit within defined Electronic Security Perimeters, that all External Routable Connectivity passes through identified access points with default-deny rules, and that Interactive Remote Access uses an Intermediate System, encryption, and multi-factor authentication. Vendor remote access must be visible and stoppable, including for associated EACMS and PACS. In NERC's 2025 list of the ten most frequently reported CIP noncompliance areas, CIP-005 ranked eighth.

From the Field

The Electronic Security Perimeter isn't a concept. It's a defined boundary, drawn on a network diagram, with specific controls at each crossing. CIP-005 expects the diagram and the controls to match. The CIP-005 problem I'd worry about first is an undocumented crossing. A connection that exists on the network but not on the perimeter diagram is a crossing the program didn't know it had.

4 CIP-006 and Physical Security Controls for Medium Impact Systems

Where CIP-005 draws the logical boundary, CIP-006 draws the physical one. The version in force is CIP-006-6, effective July 1, 2016. Physical security for medium impact systems is not secondary. Physical access can defeat logical controls, introduce malicious code through removable media, or simply disrupt the equipment.

4.1 The Physical Security Perimeter

The NERC Glossary defines the Physical Security Perimeter as 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. CIP-006-6 R1 requires one or more documented physical security plans, and the plan's content depends on whether the medium impact system has External Routable Connectivity:

- **Without External Routable Connectivity (Part 1.1).** Define operational or procedural controls to restrict physical access.
- **With External Routable Connectivity (Part 1.2).** Use at least one physical access control to allow unescorted physical access into each applicable PSP only to individuals who have authorized unescorted physical access.

The standard leaves the choice of control to the entity. A badge system, a keyed lock with controlled key issuance, or another physical access control can satisfy Part 1.2, provided the evidence shows it limits unescorted entry to authorized people.

4.2 Monitoring, Alarms, and Logs

For medium impact systems with External Routable Connectivity and their associated EACMS and PCA, CIP-006-6 also requires the entity to:

- monitor for unauthorized access through a physical access point into a PSP (Part 1.4);
- issue an alarm or alert to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detecting unauthorized access (Part 1.5);
- log the entry of each individual with authorized unescorted physical access, with information identifying the individual and the date and time of entry (Part 1.8); and
- retain those entry logs for at least ninety calendar days (Part 1.9).

Physical Access Control Systems associated with these medium impact systems must themselves be monitored for unauthorized physical access, with an alarm or alert within 15 minutes (Parts 1.6 and 1.7). For medium impact systems at Control Centers, Part 1.10 adds protection for cabling and nonprogrammable communication components that run outside a PSP within the same ESP: physical access restriction, or encryption, or link monitoring with a 15-minute alert, or an equally effective logical protection.

4.3 Visitor Control

Visitor control is a recurring focus. For medium impact systems with External Routable Connectivity, R2 requires continuous escorted access of visitors within each PSP (Part 2.1), logging of visitor entry and exit with the date and time of initial entry and last exit, the visitor's name, and the name of the point of contact responsible for the visitor (Part 2.2), and retention of visitor logs for at least ninety calendar days (Part 2.3). The escort and logging obligations both carry an exception for CIP Exceptional Circumstances.

4.4 Maintenance and Testing

For medium impact systems with External Routable Connectivity, R3 requires maintenance and testing of each Physical Access Control System, and of locally mounted hardware or devices at the PSP, at least once every 24 calendar months to ensure they function properly. A badge reader that has not been tested inside the window is a finding even if it works.

4.5 The CIP-004 Link: Who Holds Access

The list of people allowed through the perimeter belongs to CIP-004-7, effective January 1, 2024. For medium impact systems with External Routable Connectivity and their associated EACMS and PACS, CIP-004-7 requires a process to authorize electronic access and unescorted physical access based on need (Part 4.1), verification at least once each calendar quarter that individuals with active access have authorization records (Part 4.2), and, for electronic access, verification at least once every 15 calendar months that user accounts and privileges are correct and necessary (Part 4.3). On a termination action, Part 5.1 requires removal of the individual's ability for unescorted physical access and Interactive Remote Access within 24 hours.

4.6 Security and Operations at the Fence Line

Substations, Control Centers, and generating plants need access for operators, maintenance crews, and contractors. The standard does not dictate facility design. It requires that access is controlled, recorded, and reviewed. CIP-006 completes the dual perimeter that CIP-005 began: one electronic, one physical, both documented.

End-of-Chapter Summary

CIP-006-6 sets physical security plans for medium impact systems, scaled by External Routable Connectivity. Visitor control, 24-month PACS testing, and CIP-004-7 access authorization and revocation complete the physical layer.

> **From the Field**
>
> People who left the company three years ago should not have active badge credentials. When they do, the audit finds out fast.

5 CIP-007 and System Security Management for Medium Impact Systems

CIP-005 and CIP-006 protect the boundaries. CIP-007 manages what sits inside them. The version in force is CIP-007-6, effective July 1, 2016. It covers ports and services, security patch management, malicious code prevention, security event monitoring, and system access control. Its purpose is to reduce exploitable vulnerabilities inside the perimeter while giving the entity visibility into behavior that could affect reliability.

5.1 Ports and Services

Part 1.1 requires, where technically feasible, enabling only the logical network accessible ports the entity has determined are needed, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports, the open ports are deemed needed. Not every port must be closed. Every enabled port must be needed, and the entity must be able to show why. For medium impact systems at Control Centers, Part 1.2 adds protection against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.

5.2 Security Patch Management

Patching is hard in medium impact environments. Many operational technology systems cannot be taken offline to apply a patch without significant disruption. CIP-007-6 R2 handles that through process, not through a fixed patching deadline:

- **Part 2.1.** A patch management process for tracking, evaluating, and installing cyber security patches, including identification of the source or sources monitored for each applicable Cyber Asset.
- **Part 2.2.** At least once every 35 calendar days, evaluate security patches released since the last evaluation for applicability.
- **Part 2.3.** Within 35 calendar days of completing the evaluation, apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan.
- **Part 2.4.** Implement each mitigation plan within its stated timeframe, unless the CIP Senior Manager or delegate approves a revision or extension.

The audit question is whether the cycle ran on time, every time, for every source. A missed evaluation window is a violation whether or not a relevant patch was released.

5.3 Malicious Code Prevention

Part 3.1 requires methods to deter, detect, or prevent malicious code. The standard does not mandate antivirus software. Where traditional antivirus cannot run without threatening operational stability, the entity can use other methods. The measures cite traditional antivirus, system hardening, and policies as examples, and the evidence has to show the chosen method is actually performed. Part 3.2 requires mitigating the threat of detected malicious code. Part 3.3 requires a process for updating signatures or patterns, including testing and installation, for methods that use them.

5.4 Security Event Monitoring

Part 4.1 requires logging events, at the BES Cyber System or Cyber Asset level per system capability, for identification of and after-the-fact investigation of Cyber Security Incidents, including at a minimum detected successful login attempts, detected failed access and login attempts, and detected malicious code. For medium impact systems with External Routable Connectivity, Part 4.2 requires alerts for security events the entity determines necessitate an alert, including at a minimum detected malicious code and detected failure of the Part 4.1 event logging. For medium impact systems at Control Centers, Part 4.3 requires retention of the logs for at least the last 90 consecutive calendar days, where technically feasible. The 15-day log review in Part 4.4 applies to high impact only.

5.5 System Access Control

R5 supports the perimeter from the inside. For medium impact systems, the entity must identify and inventory known enabled default or generic account types (Part 5.2), change known default passwords (Part 5.4), and, for password-only authentication, enforce a minimum password length and complexity (Part 5.5). For medium impact systems with External Routable Connectivity, the entity must also identify individuals with authorized access to shared accounts (Part 5.3). Part 5.1 requires methods to enforce authentication of interactive user access, where technically feasible, for medium impact systems at Control Centers and those with External Routable Connectivity. Part 5.6 requires password changes at least once every 15 calendar months for medium impact systems with External Routable Connectivity, and Part 5.7 requires limiting unsuccessful authentication attempts or alerting on them for medium impact systems at Control Centers.

The periodic review of who has which privileges is a CIP-004 obligation (Part 4.3), not a CIP-007 one. Programs that split account management across the two standards need to make sure the hand-off is documented.

CIP-007-6 cadence	Requirement
Every 35 calendar days	Evaluate released security patches for applicability (Part 2.2)
Within 35 calendar days of evaluation	Apply, create a mitigation plan, or revise one (Part 2.3)
At least 90 consecutive calendar days	Retain event logs, medium impact at Control Centers (Part 4.3)
At least once every 15 calendar months	Change passwords, medium impact with ERC (Part 5.6)

5.6 Technical Feasibility and the Link to CIP-010

Several CIP-007 parts apply "where technically feasible." That phrase is not a blanket exemption. Under Section 411 of the NERC Rules of Procedure, a Registered Entity subject to a CIP requirement that permits Technical Feasibility Exceptions may request one, and the request is reviewed and, if approved, implemented under Appendix 4D.

CIP-007 also depends on CIP-010. The CIP-010 baseline lists the logical network accessible ports and the security patches applied, and those entries are the reference point for the CIP-007 work. When the two drift apart, both standards are at risk.

End-of-Chapter Summary

CIP-007-6 sets system security management controls for medium impact BES Cyber Systems: justified ports and services, a 35-day patch evaluation and response cycle, malicious code prevention, security event logging and alerting, and system access controls. Several parts depend on whether the system has External Routable Connectivity or sits at a Control Center, so the CIP-002 and CIP-005 scoping decisions directly shape the CIP-007 workload.

> **From the Field**
>
> CIP-007 is where most operational compliance effort lives, and it's also where findings cluster. The two facts are connected. A patch cycle runs every 35 days whether anyone is watching or not, and a single missed evaluation for a single source is enough. The programs that hold up treat the cycle as an operating process with an owner, not a quarterly cleanup.

6 CIP-010 and Configuration Change Management for Medium Impact Systems

CIP-010 formalizes a simple idea: the entity knows how its systems are configured, controls changes to that configuration, and checks the systems for vulnerabilities on a schedule. The version in force is CIP-010-4, effective October 1, 2022. Its purpose is to prevent unauthorized and unmanaged change that could degrade reliability or open a vulnerability.

6.1 The Baseline Configuration

Part 1.1 requires a baseline configuration, individually or by group, for each applicable system. The baseline must include the operating system or firmware, including version; commercially available or open-source application software, including version; custom software installed; logical network accessible ports; and any security patches applied. The baseline is not a static inventory. It is the documented current state, and every authorized change has to be reflected in it.

6.2 Configuration Change Management

The change management parts work as a sequence:

- **Part 1.2.** Authorize and document changes that deviate from the existing baseline.
- **Part 1.3.** Update the baseline as necessary within 30 calendar days of completing the change.
- **Part 1.4.** Before the change, determine the CIP-005 and CIP-007 controls that could be affected. After the change, verify those controls were not adversely affected, and document the results.
- **Part 1.6.** Before a change to the operating system or firmware, commercially available or open-source software, or security patches, verify the identity of the software source and the integrity of the software obtained, when the method to do so is available from the software source.

The standard requires documented procedures, not fixed calendars for when changes may happen. Outage scheduling, maintenance windows, and coordination with the control room remain operational decisions. CIP-010 requires that whatever change happens, it is authorized, tested against the security controls, and recorded. The 35-day configuration monitoring in Part 2.1 and the test environment requirement in Part 1.5 apply to high impact only.

6.3 Vulnerability Assessments

Part 3.1 requires a paper or active vulnerability assessment at least once every 15 calendar months for medium impact systems. Part 3.4 requires documenting the results and an action plan to remediate or mitigate the vulnerabilities identified, including the planned date for completing the action plan and the execution status of any remediation or mitigation. The 36-month active assessment in Part 3.2 and the pre-production assessment of new Cyber Assets in Part 3.3 apply to high impact only.

The assessment is a recurring obligation, and the follow-through is part of what gets audited. An assessment with findings and no dated action plan is an incomplete assessment.

6.4 Transient Cyber Assets and Removable Media

R4 requires each entity, for its high and medium impact BES Cyber Systems and associated Protected Cyber Assets, to implement one or more documented plans for Transient Cyber Assets and Removable Media that include the sections in Attachment 1. A vendor laptop connected to a network inside a medium impact ESP for an afternoon is a Transient Cyber Asset under the Glossary, and the plan has to say how its risk is managed before it connects.

6.5 Legacy Systems

Every medium impact environment has legacy equipment, some of it no longer supported by its vendor. CIP-010 says nothing about modernization. It says that whatever runs in production is baselined, that changes to it are authorized and verified, and that its vulnerabilities are assessed on cycle. An unsupported system can be compliant. An undocumented one cannot.

6.6 What Enforcement Data Shows

NERC's ORCP and CMEP Annual Report, published February 11, 2026, lists CIP-010 first among the ten most frequently reported CIP noncompliance areas in 2025. The report also explains a practice that matters here. No current CIP requirement says to identify PACS, PCA, or EACMS, yet missing one can violate several requirements at once. The ERO Enterprise processes that failure as a single CIP-010 R1 violation, pending a permanent fix through standards development.

End-of-Chapter Summary

CIP-010-4 requires medium impact baselines, controlled and verified changes with baseline updates within 30 calendar days, 15-month vulnerability assessments with dated action plans, and Transient Cyber Asset and Removable Media plans. It tops NERC's 2025 list of reported CIP noncompliance.

> **From the Field**
>
> A change made without going through the change process is a change the audit will find. The vulnerability assessment isn't a one-time scan. The recurrence is part of what gets audited.

7 CIP-011, Information Protection, and Data Integrity

CIP-011 protects the information about BES Cyber Systems. The version in force is CIP-011-3, effective January 1, 2024. For medium impact systems and their associated EACMS and PACS, it extends protection from the devices and networks to the information that describes how they are built and secured.

7.1 What Counts as BCSI

The NERC Glossary defines BES Cyber System Information as information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the system. The definition excludes individual pieces of information that by themselves pose no threat, such as device names, individual IP addresses without context, ESP names, or policy statements. Its examples include security procedures or security information about BES Cyber Systems, PACS, and EACMS that is not publicly available, collections of network addresses, and network topology of the BES Cyber System.

7.2 The Information Protection Program

R1 requires one or more documented information protection programs. Part 1.1 requires methods to identify BCSI. Part 1.2 requires methods to protect and securely handle BCSI to mitigate risks of compromising confidentiality. Part 1.2 asks the entity to mitigate risk, not eliminate it. It requires that the identification and protection methods are defined, implemented, and applied consistently to the information the entity has identified.

Storage location now matters more than it used to. The CIP-011-3 measures give separate evidence examples for on-premise and off-premise BCSI, and NERC's 2025 annual report notes that the ERO Enterprise confirmed a uniform understanding of the endorsed Implementation Guidance on cloud solutions for BCSI under CIP-004-7 R6 and CIP-011-3 R1.

7.3 Reuse and Disposal

R2 covers the end of an asset's life. Before releasing an applicable Cyber Asset that contains BCSI for reuse, other than reuse within other applicable systems, the entity must take action to prevent unauthorized retrieval of BCSI from its data storage media (Part 2.1). Before disposal, it must take action to prevent unauthorized retrieval of BCSI from the Cyber Asset or destroy the data storage media (Part 2.2). Sanitization or destruction records are the evidence.

7.4 Information in the Layered Architecture

Information protection ties directly to the other standards. The network diagrams that define the ESP under CIP-005, the baselines under CIP-010, and the rule sets behind CIP-007 and CIP-

005 are all likely BCSI. Medium impact sites share technical information with vendors, contractors, and affiliates as a matter of routine, and the program has to say how that sharing is controlled.

The logic is straightforward. The more an adversary knows about a system's configuration, security features, and operations, the easier it is to exploit. Protecting the information complements the electronic and physical perimeters by denying an attacker the map.

End-of-Chapter Summary

CIP-011-3 requires medium impact entities to identify BCSI, protect and securely handle it wherever it is stored, and prevent its unauthorized retrieval when Cyber Assets are reused or disposed of. It brings the information that describes the system under the same layered architecture that protects the system itself.

> **From the Field**
>
> BES Cyber System Information is the data about the system. Protecting it is part of protecting the system, because the data describes how to compromise the system. A network diagram emailed to a vendor unencrypted is a CIP-011 finding waiting to happen. The boundaries of CIP-011 are wider than most programs first assume, and the program has to think clearly about scope.

8 CIP-008 and CIP-009: Incident Response and Recovery for Medium Impact Systems

The medium impact control architecture assumes preventive controls will not be fully effective. CIP-008 and CIP-009 build the capability to respond to a Cyber Security Incident and to recover the affected systems. Both apply to high and medium impact BES Cyber Systems.

8.1 The Incident Response Plan

CIP-008-6, effective January 1, 2021, requires one or more documented Cyber Security Incident response plans. R1 requires processes to identify, classify, and respond to Cyber Security Incidents (Part 1.1); processes that include criteria to evaluate and define attempts to compromise, and that determine whether an identified incident is a Reportable Cyber Security Incident or an attempt to compromise an applicable system (Part 1.2); defined roles and responsibilities of response groups or individuals (Part 1.3); and incident handling procedures (Part 1.4).

The Glossary sets the scope. For a medium impact system, a Cyber Security Incident is a malicious act or suspicious event that compromises or attempts to compromise an ESP, a PSP, or an EACMS, or that disrupts or attempts to disrupt a BES Cyber System. The Reportable Cyber Security Incident definition appears in the Glossary at the back of this reference.

8.2 Testing and Updating the Plan

R2 requires testing each plan 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. R3 requires, no later than 90 calendar days after a test or actual Reportable Cyber Security Incident response, documenting lessons learned (or their absence), updating the plan, and notifying each person or group with a defined role. A change to roles, response groups, or technology that would affect the ability to execute the plan triggers the same update and notification within 60 calendar days.

8.3 Notification Deadlines

R4 requires notifying the Electricity Information Sharing and Analysis Center (E-ISAC) and, for entities subject to U.S. jurisdiction, the National Cybersecurity and Communications Integration Center (NCCIC) or their successors. Initial notification is due within one hour after determining that a Reportable Cyber Security Incident occurred, and by the end of the next calendar day after determining that an incident was an attempt to compromise an applicable system. Notifications must include, to the extent known, the functional impact, the attack vector, and the

level of intrusion achieved or attempted. Updates are due within 7 calendar days of determining new or changed information.

The determination is the obligation. Apply the documented criteria and record the decision, including a decision not to report. An undocumented judgment call is hard to defend later.

8.4 Recovery Plans

CIP-009-6, effective July 1, 2016, requires one or more documented recovery plans for medium impact BES Cyber Systems. Each plan must include the conditions for activation (Part 1.1), the roles and responsibilities of responders (Part 1.2), processes for backup and storage of information required to recover functionality (Part 1.3), and processes to preserve data, per Cyber Asset capability, for determining the cause of a Cyber Security Incident that triggers the plan, without impeding recovery (Part 1.5). For medium impact systems at Control Centers, Part 1.4 adds processes to verify the successful completion of backups and to address backup failures.

8.5 Testing Recovery

For medium impact systems at Control Centers, R2 requires testing each recovery plan at least once every 15 calendar months, through recovery from an actual incident, a paper drill or tabletop, or an operational exercise (Part 2.1), and testing a representative sample of backup information at least once every 15 calendar months to confirm it is usable and compatible with current configurations (Part 2.2). The 36-month operational exercise in Part 2.3 applies to high impact only. For the same systems, R3 requires documenting lessons learned and updating the plan within 90 calendar days after a test or actual recovery, and updating it within 60 calendar days after relevant changes. Medium impact systems outside Control Centers still need a recovery plan under R1, even though the R2 testing and R3 update parts do not reach them.

8.6 Response Inside Real Operations

When a Cyber Security Incident hits a medium impact control system, the response touches operations. The standards define processes and roles, not how the system is operated during the incident. That coordination with operating personnel belongs in the plan, written before it is needed.

End-of-Chapter Summary

CIP-008-6 and CIP-009-6 require medium impact entities to plan for, test, and report Cyber Security Incidents and to recover afterward, on 15-month test cycles and a one-hour reporting clock.

> **From the Field**
>
> CIP-008 and CIP-009 assume prevention will fail. Programs designed only for prevention are designed for the wrong scenario. The real test is whether the people named in the plan know they're named.

9 Oversight, Audit Posture, and Enforcement Trends for Medium Impact Systems

Medium impact BES Cyber Systems draw sustained attention from the ERO Enterprise. This chapter explains how audits of the tier are scoped and run, what RSAWs do and do not do, and what NERC's most recent annual data says about where programs fail.

9.1 How Audits Are Scoped

Under Appendix 4C of the NERC Rules of Procedure, the Compliance Enforcement Authority tailors the scope of a Compliance Audit to Reliability Standards identified through NERC-approved risk-based processes, including Inherent Risk Assessments, internal controls, and other inputs. An entity whose functional profile, system design, or compliance history presents higher risk can expect a deeper technical review.

The notice tells you a great deal. Appendix 4C requires the Compliance Enforcement Authority to notify the Registered Entity at least 270 days before a planned Compliance Audit, and at least 90 days before a scheduled audit to identify the Reliability Standards to be evaluated, the audit team members and their recent employment history, and the documents, data, and information requested.

9.2 What Auditors Ask For

Medium impact audits combine document review, technical interviews, configuration validation, and sampling of implementation evidence. Expect requests for ESP network diagrams, baselines, access rule sets, patch evaluation records, access authorization and revocation records, vulnerability assessment reports, and incident response test records. The ERO Enterprise's CIP Evidence Request Tool, with its published user guide, structures much of that request around detail tabs for BES assets, Cyber Assets, ESPs, EAPs, PSPs, Transient Cyber Assets, Removable Media, BCSI, personnel, reuse and disposal, Cyber Security Incidents, and procurement. The common thread is simple. The auditor is testing whether the documented process reflects the actual state of the system.

9.3 What RSAWs Are

NERC describes a Reliability Standard Audit Worksheet as a guide that describes types of evidence registered entities may use to demonstrate compliance with a Reliability Standard, along with information on how the ERO may assess that evidence. RSAWs do not require specific evidence, are not intended to require a single approach to assessing compliance, and may not be used to change the scope or intent of a Reliability Standard. They are a strong

preparation tool for that reason: they show the evidence categories an audit team will look for, such as access review records, change approvals, vulnerability assessment reports, and media sanitization records, without adding obligations the standard does not contain.

9.4 What the 2025 Data Shows

NERC's ORCP and CMEP Annual Report, published February 11, 2026, gives the most current picture. In 2025 the most frequently reported CIP noncompliance involved CIP-010, CIP-007, and CIP-004, all of which, in NERC's words, involve high-volume and high-frequency conduct. The report identifies lack of or deficient policies and procedures as the leading root cause for all three. The full top ten, in the report's order, was CIP-010, CIP-007, CIP-004, CIP-003, CIP-006, CIP-011, CIP-002, CIP-005, CIP-009, and CIP-013.

The same report states that registered entities self-identified approximately 85% of reported noncompliance in 2025. For a medium impact program, the lesson is that internal detection is the norm the ERO Enterprise expects. A program that finds its own missed patch cycle and reports it is in a very different position from one whose auditor finds it first.

9.5 Technical Feasibility and Consistency

Medium impact environments are always on, and an audit of them does not require taking control systems down. It does require enough validation to show that controls are in place and that procedures are followed. Where a requirement allows it and a control cannot be implemented as written, the Technical Feasibility Exception process under Section 411 and Appendix 4D of the Rules of Procedure is the route, and an approved exception is part of the evidence package.

End-of-Chapter Summary

Regional Entity oversight of medium impact BES Cyber Systems is risk-based and scoped through Inherent Risk Assessments, internal controls, and other inputs. RSAWs describe the evidence an audit team will look for without changing the standard. NERC's 2025 data puts CIP-010, CIP-007, and CIP-004 at the top of reported CIP noncompliance, with deficient policies and procedures as the leading cause.

> **From the Field**
>
> The Region tells you what they're going to look at, in the audit notice. Programs that read the notice carefully and prepare specifically rarely get surprised. NERC's 2024 and 2025 annual reports put the same three CIP standards at the top of reported noncompliance. Knowing the cluster is most of the preparation.

10 Medium Impact Systems and the Operational Reliability Interface

Medium impact BES Cyber Systems sit where cybersecurity governance meets real-time control. Control Centers, generation control systems, substation automation, and the networks that connect them are not abstract IT environments. They support frequency control, voltage management, contingency response, and restoration. The medium impact framework has to coexist with those duties.

10.1 Availability First

Operational technology environments prioritize availability and deterministic performance. Control systems often run continuously and may not tolerate frequent reboots, intrusive scanning, or unplanned configuration changes. The medium impact standards recognize that by relying on documented processes, risk evaluation, and justified exceptions rather than rigid technical prescriptions. The enforceable expectation is disciplined governance that keeps the system running.

10.2 Controls Inside Operating Authority

Cybersecurity controls have to fit the operating structure. Multi-factor authentication for Interactive Remote Access under CIP-005 must work when an engineer needs to troubleshoot quickly. The 35-day patch cycle under CIP-007 has to account for maintenance windows and coordination with operations. Configuration change management under CIP-010 has to align with outage scheduling. None of these requirements tells operators how to run the system. All of them require the security process to run inside the operating process, not around it.

10.3 Incident Response as an Operating Event

The interface is sharpest during an incident. A Cyber Security Incident affecting a medium impact control system may require coordination among security staff, operators, and reliability leadership. Decisions to isolate a system, sequence its restoration, or operate around it must balance containment against system stability. The standards do not prescribe those tactical decisions. They require defined processes and documented authority, so the decision is made by the right person on the right basis.

10.4 Operationally Significant, Not High Impact

The criteria that rate a facility medium impact, such as 1,500 MW of shared generation, 500 kV transmission, IROL-critical facilities, and Transmission Operator Control Centers, describe assets that matter in contingency analysis and restoration. They are operationally significant even though CIP-002 does not rate them high. The control depth of the medium tier reflects that relevance.

10.5 One Architecture, Many Layers

Taken together, the medium impact standards form one structure: governance under CIP-003, personnel and access under CIP-004, the electronic perimeter under CIP-005, physical protection under CIP-006, system security management under CIP-007, response and recovery under CIP-008 and CIP-009, configuration discipline under CIP-010, information protection under CIP-011, and supply chain risk management under CIP-013. Each layer addresses a distinct path to compromise. The balance the framework strikes is that security reinforces control authority rather than impairing it.

Many of the cycles line up on 15 calendar months, which gives a program a natural annual rhythm with a cushion:

15-month obligation	Standard and requirement
Review and approve BES Cyber System identifications	CIP-002-5.1a R2
Review and approve cyber security policies	CIP-003-9 R1
Verify user accounts and privileges	CIP-004-7 Part 4.3
Change passwords, medium impact with ERC	CIP-007-6 Part 5.6
Conduct a paper or active vulnerability assessment	CIP-010-4 Part 3.1
Test the incident response plan	CIP-008-6 Part 2.1
Test recovery plans and backups, medium impact at Control Centers	CIP-009-6 Parts 2.1 and 2.2
Review and approve the supply chain risk management plan	CIP-013-2 R3

10.6 Change Keeps Coming

Automation, remote monitoring, and the integration of new resources keep adding connectivity paths. As architectures change, the medium impact classification and its controls have to be applied consistently to each new configuration. The standards provide the mechanism: the 15-month CIP-002 review and the CIP-010 baseline update on every authorized change. The durability of the framework depends on cybersecurity being part of reliability governance, not an overlay on top of it.

End-of-Chapter Summary

Medium impact BES Cyber Systems operate at the intersection of cybersecurity governance and real-time operational control. The layered CIP architecture protects operational technology while preserving availability and operating authority. Through risk-based classification and integrated control requirements, the medium impact framework embeds cyber resilience within Bulk Electric System reliability.

11 What Changes Next: Approved Revisions for 2028 and 2029

Every requirement cited so far is in force in October 2026. Several approved revisions will change the medium impact program before the end of the decade. Programs that plan for them now will absorb them on their own schedule rather than the deadline's.

11.1 The Virtualization Revisions

NERC's standards listing shows a family of revised CIP standards subject to future enforcement on July 1, 2028: 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. They come from Project 2016-02, Modifications to CIP Standards, which addresses virtualization. The revised Glossary definitions that take effect with them (FERC docket RM24-8-000) extend core terms to virtual environments. A BES Cyber Asset, for example, becomes "a Cyber Asset or Virtual Cyber Asset" meeting the 15-minute impact test, and the Cyber Asset definition excludes Shared Cyber Infrastructure. CIP-002-7 never takes effect; FERC approved its retirement immediately prior to the effective date of CIP-002-8 (Docket No. RD25-8-000).

For a medium impact program running virtualized servers, hypervisors, or software-defined networking, the inventory and categorization work starts well before 2028.

11.2 CIP-002-8 and Control Center Categorization

FERC approved CIP-002-8 and a revised Control Center definition in an order issued March 19, 2026 in Docket RD25-8-000. The revised definition reaches Transmission Owners that can control transmission Facilities at two or more locations through SCADA. Criterion 2.12 now assigns weighted points to the BES Transmission Lines a Control Center monitors and controls, with a threshold of 6,000 aggregate weighted points separating medium from low impact for Control Centers of Transmission Operators and Transmission Owners. The NERC listing shows CIP-002-8 subject to future enforcement on July 1, 2028.

11.3 Internal Network Security Monitoring

CIP-015-1 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. The processes must implement risk-based network data feeds, methods to detect anomalous network activity, and methods to evaluate what is detected. NERC lists CIP-015-1 as subject to future enforcement on October 1, 2028. CIP-015-2, listed for October 1, 2029, extends the monitoring obligation to the EACMS, PACS, and PCA associated with those systems and supporting Shared Cyber Infrastructure.

11.4 Low Impact Changes and Medium Impact Programs

CIP-003-11, subject to future enforcement on July 1, 2029, revises the low impact plan requirements. It does not change the medium impact policy topics in R1, but most entities with medium impact systems also own low impact assets, and the same governance team usually runs both.

Standard	Effect on medium impact programs	Subject to enforcement
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, CIP-013-3	Virtualization revisions across the family	July 1, 2028
CIP-002-8	Revised Control Center definition and criterion 2.12 (supersedes CIP-002-7, retired before it takes effect)	July 1, 2028
CIP-015-1	Internal network security monitoring inside medium impact ESPs with ERC	October 1, 2028
CIP-015-2	Extends monitoring to associated EACMS, PACS, and PCA and supporting Shared Cyber Infrastructure	October 1, 2029
CIP-003-11	Low impact plan revisions	July 1, 2029

End-of-Chapter Summary

The medium impact requirements will change on July 1, 2028, when the virtualization revisions and CIP-002-8 take effect, and again with internal network security monitoring under CIP-015-1 on October 1, 2028 and CIP-015-2 on October 1, 2029. Inventory, categorization, and network monitoring design for those changes should begin well ahead of the dates.

Glossary

The following terms are defined in the NERC Glossary of Terms. Definitions are quoted from the version subject to enforcement in October 2026; several are revised by the virtualization changes effective July 1, 2028. Readers should consult the current official Glossary for authoritative language.

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.
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.
Cyber Assets	Programmable electronic devices, including the hardware, software, and data in those devices.
Electronic Access Point (EAP)	A Cyber Asset interface on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.
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.
Interactive Remote Access	User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Interactive remote access 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.

Term	Meaning in this paper
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.

The Interactive Remote Access entry omits the definition's list of the three kinds of originating Cyber Assets, which are those used or owned by the Responsible Entity, by employees, or by vendors, contractors, or consultants.

How Energy Compliance Can Help

Medium impact programs hold up or fail on the categorization behind them and on evidence that keeps pace with the 35-day and 15-month cycles. Every deliverable is structured for the auditor's question, not the consultant's binder: operationally executable in real time, audit-defensible at compliance review. 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

For a medium impact program, the closest fits are the classification and boundary reviews above, RSAW production and data request strategy ahead of a CIP audit, and audit defense with Notice of Penalty response and settlement posture. Around that core, EC provides NERC compliance program support, interpretation, and audit preparation; senior advisory with direct engagement 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 runs the medium impact 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, every routable operations-data path out of a plant is one the CIP-002 and CIP-005 determinations have to account for.

Start with your CIP-002 determination. If you can't tie every medium impact rating to a specific Attachment 1 criterion 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.

Our work supports registered entities, including Generator Owners and Operators, Transmission Owners and Operators, Reliability Coordinators, Balancing Authorities, and Distribution Providers. We work across 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 don't staff for billable hours. We staff for outcomes. Our deliverables are written to be operationally executable and audit-defensible, not to manufacture activity. 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

- NERC Reliability Standard CIP-002-5.1a, Cyber Security, BES Cyber System Categorization (Attachment 1 Impact Rating Criteria). 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. 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-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-015-1, Cyber Security, Internal Network Security Monitoring. https://www.nerc.com/globalassets/standards/reliability-standards/cip/cip-015-1.pdf

- NERC Reliability Standard CIP-015-2, Cyber Security, Internal Network Security Monitoring. https://www.nerc.com/globalassets/standards/reliability-standards/cip/cip-015-2.pdf
- NERC, Reliability Standards, CIP family listing (versions, enforcement status, and effective dates), retrieved October 25, 2026. https://www.nerc.com/standards/reliability-standards/cip
- NERC, Project 2016-02 Modifications to CIP Standards, Implementation Plan (clean, April 3, 2024). https://www.nerc.com/globalassets/standards/reliability-standards/cip/2016-02-virtualization-implementation-plan_clean_04032024.pdf
- FERC, Order Approving Reliability Standard CIP-002-8, Docket No. RD25-8-000 (issued March 19, 2026), 91 Fed. Reg. 14013 (March 24, 2026), FR Doc. 2026-05715. https://www.govinfo.gov/content/pkg/FR-2026-03-24/pdf/2026-05715.pdf
- NERC, Glossary of Terms Used in NERC Reliability Standards. https://www.nerc.com/glossary-of-terms
- NERC, 2024 CMEP and ORCP Annual Report (February 2025). https://nerc.com/pa/comp/CE/ReportsDL/2024%20CMEP%20and%20ORCP%20Annual%20Report.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 Rules of Procedure, Section 411, Requests for Technical Feasibility Exceptions to NERC Critical Infrastructure Protection Reliability Standards (effective November 28, 2023). https://www.nerc.com/globalassets/who-we-are/rules-of-procedure/nerc-rop.pdf
- NERC Rules of Procedure, Appendix 4D, Procedure for Requesting and Receiving Technical Feasibility Exceptions to NERC CIP Standards (effective July 1, 2016). https://www.nerc.com/globalassets/who-we-are/rules-of-procedure/appendix-4d.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, Reliability Standard Audit Worksheet (RSAW) Review and Revision Process (effective March 1, 2018). https://www.nerc.com/globalassets/programs/compliance/rsaws/nerc-reliability-standard-audit-worksheet-rsaw-review-and-revision-process.pdf
- 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

© Energy Compliance, Inc. · EC-WP-202 · October 2026