CYBERSECURITY · CIP SERIES · EC-WP-205

Cyber Reliability at T&D Interfaces

Where regulated cybersecurity meets mostly unregulated cybersecurity, and shared risk concentrates.

At the seam between transmission and distribution, CIP applies on one side and mostly does not apply on the other. The risk crosses anyway, through shared substations, data feeds, remote access and common services. This reference explains where the federal obligation starts and stops, where the standards do assign duties across the seam, and what a program has to manage on its own. It reflects the requirements in force in October 2026 and the CIP changes already approved through 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

The transmission and distribution interface is where regulated cybersecurity meets mostly unregulated cybersecurity. Section 215 of the Federal Power Act limits NERC's standards to the bulk-power system and leaves out facilities used in the local distribution of electric energy. CIP therefore applies on the transmission side. On the distribution side it reaches only a short list of systems that Distribution Providers own for the protection or restoration of the BES: qualifying load shedding systems, Remedial Action Schemes, transmission Protection Systems, and Cranking Path elements. Everything else on that side is managed by the utility and, where a state chooses to act, by state regulators. It is not federally audited.

The seam is where shared risk concentrates. Substations serve both systems. Data flows both ways, and the NERC standards themselves require some of it: TOP-003-7, in effect since October 1, 2026, tells each Transmission Operator to specify the non-BES data it needs and obliges Distribution Providers that receive the specification to deliver it by a mutually agreeable secure method. Remote access, shared networks and common IT services connect the two sides in ways the scope documents don't show.

The points below are my own read of the interface. Each is developed, with its sources, in the chapters that follow.

- Cyber risk doesn't respect the BES/non-BES line. Adversaries don't read the NERC scope document.
- The seam between regulated and unregulated is where the most unmonitored risk lives. Knowing what crosses the seam matters more than knowing what's on each side.
- A breach that starts outside scope is still judged inside scope by one test: did the in-scope controls it passed through meet the requirement?
- Smart grid integration brought T&D operations closer than the historical scope language anticipated. The standards are catching up: CIP-012-2 took effect July 1, 2026, CIP-002-8 extends the Control Center definition to certain Transmission Owner SCADA facilities on July 1, 2028, and internal network security monitoring arrives with CIP-015-1 on October 1, 2028.
- Two utilities can share a risk surface and have little shared regulatory obligation to manage it. Operationally that gap has to be closed even where the standards don't require it.
- Defense-in-depth at the interface is a program decision, not a regulatory one. The standard tells you the floor; the threat environment tells you the ceiling.

1 Defining Cybersecurity Reliability at the Transmission and Distribution Interface

This chapter sets the terms. Two questions get asked about every system at the interface, and they have different answers: is it in scope, and can it hurt the grid?

1.1 Compliance Scope and Reliability Risk Are Different Questions

In this reference, cybersecurity reliability means the ability of connected cyber and physical systems to keep delivering power reliably while under cyber threat, and to recover when something gets through. It is not the same as being compliant with the CIP standards for a particular set of assets. Compliance asks whether a registered entity met the requirements that apply to the systems in its scope. Cybersecurity reliability asks what the cyber environment does to system performance, to operating decisions, and to the wider grid.

The two questions overlap, but they draw different maps. The compliance map follows the statute, the BES definition and the applicability sections of the standards. The risk map follows networks, data feeds, trust relationships and people. At the transmission and distribution interface those maps diverge more than anywhere else.

1.2 What the Interface Is

The interface has a physical side and a functional side. Physically, it is the substations, Protection Systems and control equipment at the points where transmission and distribution connect. Many substations hold both: transmission Elements on one bus, distribution feeders on another, and one control house, one network and one set of relay engineers serving both.

Functionally, it is the data and control exchanged across that boundary. Breaker status, voltage and flow data move from distribution to transmission operators and back. Load shedding schemes, protection coordination and restoration switching tie the two systems together in time. None of this changes the legal line, but all of it carries risk across it.

1.3 Responsibility, Obligation and Risk

The difficulty at this boundary is separating three things that people tend to blur. Risk is shared: a compromised system on either side can affect the other. Obligation is not generally shared: the NERC standards assign requirements to registered functions, and most distribution systems have none. Responsibility sits with whoever owns and operates each system, whatever its regulatory status.

The reliability framework therefore works with two maps at once. One defines where mandatory requirements apply. The other describes where risk can arise and where it can be transferred. A program that manages only the first map is compliant. A program that manages both is the one I'd want running the system.

1.4 Why the Interface Has Changed

Distribution systems were historically built as radial, customer-facing networks with few connections to the bulk system, while transmission required wide-area coordination from a central point. That separation has narrowed. Distribution automation, distributed energy resources and shared communications have pulled the two sides closer, and the data that crosses the boundary now matters to real-time decisions in a way it did not when the scope language was written.

That is my view of the trend, not a regulatory finding. The standards have responded in specific places, which later chapters cover. The interface has not disappeared. What has changed is the coupling across it, and the coupling is what has to be understood.

1.5 What This Reference Does and Does Not Do

This reference explains boundaries, shared risk and oversight as they stand in the current reliability and cybersecurity standards. It does not prescribe controls or substitute for an entity's own scoping analysis. Where I offer a judgment, I label it as mine.

> **End-of-Chapter Summary**
>
> Cybersecurity reliability at the interface is about how cyber conditions affect the BES and the systems connected to it, across a formal BES/non-BES line. Compliance with the scope definitions is one factor. Risk can still move through shared resources and operating relationships. Telling compliance and risk apart is the first step.

> **From the Field**
>
> The reliability framework has to think about what happens when an attack crosses the boundary the regulation drew.
>
> The transmission and distribution interface is the seam where regulated cybersecurity meets mostly unregulated cybersecurity. Many utilities operate both sides; few coordinate them as a single risk surface.
>
> A finding on a CIP-regulated asset can trace back to an unregulated distribution system that wasn't audited. Scope doesn't equal risk, and the program has to manage both.

2 BES and Non-BES System Boundaries and Classification Concepts

The BES versus non-BES distinction is the core of the North American reliability program. It determines which facilities the Reliability Standards reach and where the CIP standards can apply at all. This chapter walks the line from the statute down to CIP-002.

2.1 The Statutory Line

Section 215 of the Federal Power Act (16 U.S.C. 824o) defines the bulk-power system as the facilities and control systems necessary for operating an interconnected transmission network, plus the generation needed to maintain transmission reliability. The definition expressly does not include facilities used in the local distribution of electric energy. The Electric Reliability Organization may develop and enforce standards only for the bulk-power system, and the statute preserves each state's authority to act for the safety, adequacy and reliability of electric service within the state, so long as the state action is not inconsistent with a Reliability Standard.

That is the legal origin of the interface. Everything else in this chapter implements it.

2.2 The BES Definition

The NERC Glossary turns the statute into a bright line. The Bulk Electric System is, unless modified by the listed inclusions and exclusions, 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.

Element	What it does at the interface
I1	Brings in transformers with the primary terminal and at least one secondary terminal at 100 kV or higher, unless E1 or E3 applies
I2 and I4	Bring in generating resources (above 20 MVA individual or 75 MVA aggregate nameplate) and dispersed power producing resources (above 75 MVA aggregate) connected at 100 kV or above
I3	Brings in Blackstart Resources identified in the Transmission Operator's restoration plan
I5	Brings in dedicated reactive devices connected at 100 kV or higher
E1	Excludes radial systems from a single point of connection at 100 kV or higher that only serve Load, or serve Load with limited non-retail generation (75 MVA or less)

Element	What it does at the interface
E2	Excludes certain behind-the-meter generation with net capacity to the BES of 75 MVA or less
E3	Excludes local networks under 300 kV that distribute power to Load rather than transfer bulk power, subject to the generation, flow and Flowgate conditions
E4	Excludes reactive devices installed for the sole benefit of a retail customer

E1 and E3 do most of the work at the T&D boundary. A 115 kV radial line serving only load is out. A 138 kV local network meeting every E3 condition is out. A transformer stepping 230 kV down to 69 kV for distribution is generally outside I1, because its secondary is below 100 kV. Each of those calls is a scope decision with cyber consequences, because the CIP standards follow the BES.

2.3 The Exception Process

The definition notes that Elements may be included or excluded case by case through the Rules of Procedure exception process. Appendix 5C, effective January 19, 2021, sets that process. The owner of an Element, or a Regional Entity, may request exclusion. A Regional Entity, Planning Authority, Reliability Coordinator, Transmission Operator, Transmission Planner or Balancing Authority with the Element in its scope may request inclusion after conferring with the owner. The Regional Entity reviews the request and recommends, and NERC approves or disapproves.

An exception changes BES status. It does not, on its own, change anyone's cyber risk.

2.4 Where Distribution Enters the Registry

Distribution Provider is a registered function. The Glossary defines it as the entity that provides and operates the "wires" between the transmission system and the end-use customer, at any voltage. Where customers are served at transmission voltage, the Transmission Owner also serves as the Distribution Provider.

Appendix 5B of the Rules of Procedure (Revision 8, effective June 27, 2024) limits registration to Distribution Providers that meet at least one criterion:

- a system serving more than 75 MW of peak Load directly connected to the BES;
- ownership, control or operation of Facilities in a required UVLS program, a required Special Protection System or Remedial Action Scheme, or a required transmission Protection System;
- services related to Nuclear Plant Interface Requirements under an executed agreement; or
- field switching personnel performing unique tasks in the Transmission Operator's restoration plan.

A separate UFLS-Only Distribution Provider category covers entities whose only qualifying assets are UFLS Protection Systems in a required UFLS program. Beyond PRC-005, PRC-006 and regional UFLS program standards, a standard applies to that category only where its applicability section names it.

2.5 From BES Status to CIP Scope

CIP-002-5.1a is where boundary logic becomes cyber scope. It applies to Distribution Providers only for four kinds of systems they own for the protection or restoration of the BES:

1. UFLS or UVLS systems in a load shedding program subject to a NERC or Regional standard that shed 300 MW or more automatically under a common control system;
2. Special Protection Systems or Remedial Action Schemes subject to a NERC or Regional standard;
3. Protection Systems, other than UFLS and UVLS, that apply to Transmission and are subject to a standard; and
4. Cranking Paths and Elements meeting the initial switching requirements from a Blackstart Resource.

Section 4.2.3.4 then exempts, for Distribution Providers, all other systems and equipment. The standard's guidance notes that a Distribution Provider may have BES Cyber Systems to scope in if it owns Elements that are part of a Cranking Path in the Transmission Operator's restoration plan.

These classifications are binary. A system is in scope for a requirement or it isn't, and that is what makes the standard enforceable. Being out of scope does not make a system safe or unimportant. It means the mandatory requirements stop there and the entity's own risk management takes over. Misreading the line goes wrong in both directions. Treating every interface system as if it carried full CIP obligations blurs accountability. Ignoring interface risk because a system is out of scope leaves the in-scope side exposed.

End-of-Chapter Summary

The BES and non-BES classifications set the scope of mandatory reliability and cybersecurity standards through a statute, a bright-line definition, an exception process and the applicability sections of each standard. They settle the obligation. They do not remove the risk that remains for systems that interface with the BES. Knowing exactly how the line is drawn is what makes an honest assessment of shared risk possible.

From the Field

The BES definition draws the line between regulated and unregulated. The line was drawn for reliability purposes, not cybersecurity ones.

A cyber path that starts outside the BES and enters an asset with BES Cyber Systems is CIP-relevant at the point where it crosses in, even if its origin is outside the framework. Programs that treat the boundary as a firewall miss the connections the boundary actually has.

3 Operational and Cyber Interdependencies Across the Interface

Interdependence does not move the legal boundary. It changes how a cyber incident or an abnormal condition on one side shows up on the other, and how fast each side can detect and respond to it.

3.1 Operational Interdependence

Transmission and distribution depend on each other in real time. Load dynamics, DER output and protection operations on the distribution side affect transmission performance. Transmission disturbances affect distribution reliability and restoration. The standards build some of that dependence directly into the system:

- **Load shedding.** UFLS and UVLS programs are designed for the protection of the BES, and much of the equipment that executes them sits on distribution systems. Appendix 5B registers the entities that own it.
- **Restoration.** A Transmission Operator's restoration plan can rely on distribution-owned Elements in a Cranking Path, and on distribution field switching personnel.
- **Protection coordination.** Transmission and distribution protection must be coordinated to avoid unnecessary outages. Where protection settings, monitoring and coordination run through cyber systems, the cyber exposure of one side reaches the other.

3.2 Data Interdependence

Operators on each side use data from the other. Transmission Operators use distribution-level data in Real-time Assessments. Distribution operators use transmission data to make feeder operation and restoration decisions. The NERC Glossary defines a Real-time Assessment as an evaluation of system conditions using Real-time data, and notes that it may be provided through internal systems or through third-party services. Data from outside the BES and outside the entity can be an input to that assessment.

TOP-003-7 and IRO-010-5 say so in terms. Each requires the Transmission Operator or Reliability Coordinator to specify the data it needs, including non-BES data and external network data, and to identify the entities responsible for providing it. Chapter 4 covers what that means for security.

3.3 Shared Communications and Shared Services

Fiber networks, leased circuits, microwave paths and data centers often serve both transmission and distribution functions. An outage or compromise of a shared resource can take

out visibility and control on both sides at once. When that happens, how concentrated the dependency is matters more to reliability than how each affected system was classified.

Organizational links add a further layer. Transmission and distribution businesses within one company often share identity services, security operations, vendor-managed applications and support staff. The reliability framework assigns responsibility for specific functions. It does not prevent these shared dependencies, and it does not account for them. A shared service that slows the detection, reporting or correction of a problem slows it for both sides.

3.4 The Dependencies Nobody Wrote Down

In my view, the most dangerous interdependencies are the unrecorded ones: a data flow set up years ago and never documented, a service account used by both sides, a shared historian, a vendor connection that outlived the project it was built for. They escape design reviews and planning, and they surface during a cyberattack or a system failure. Finding them before an adversary does is the most valuable interface work a program can do.

End-of-Chapter Summary

Transmission and distribution are tied together through operational coordination, required data exchange, common infrastructure and shared organizations. Those ties are how a vulnerability on one side can affect reliability on the other. Understanding them is the basis for managing shared risk while keeping the distinctions of responsibility and jurisdiction intact.

4 Data Exchange, Visibility, and Control Pathways

Every data exchange across the interface is also a pathway. This chapter covers what the standards require to cross, how they treat its security, and where control influence reaches across the line.

4.1 What Has to Cross

Most of the data a Transmission Operator needs comes from BES facilities, but not all of it. Distribution systems with unusual load patterns or high DER penetration can matter to transmission operations, and the standards recognize it.

Requirement	What it does at the interface
TOP-003-7 R1.1	Transmission Operator's data specification must list the data it needs for Operational Planning Analyses, Real-time monitoring and Real-time Assessments, including non-BES data, and identify who provides it
TOP-003-7 R1.5.5	The specification must include mutually agreeable methods for securely transferring the data
TOP-003-7 R3	Transmission Operator must distribute the specification to the entities that hold the data
TOP-003-7 R5	Each Distribution Provider (and other listed entity) receiving a specification must satisfy it
IRO-010-5 R1	Parallel obligation for the Reliability Coordinator's data specification, also including non-BES data and secure transfer methods

TOP-003-7 became effective October 1, 2026. IRO-010-5 is in effect. TOP-003-8 and IRO-010-6 are both approved for April 1, 2029.

4.2 Securing the Transfer

TOP-003-7 requires that the transfer method be secure and mutually agreed, but it does not define the controls. The parties decide. That makes the data specification one of the few places where the standards push the two sides of the interface into a written security agreement, and in my view it is underused for that purpose.

Between Control Centers, CIP-012-2 goes further. Effective July 1, 2026, it requires a documented plan to mitigate the risks of unauthorized disclosure, unauthorized modification and loss of availability of Real-time Assessment and Real-time monitoring data while it is transmitted between Control Centers, including methods for recovering the communication links. Where the Control Centers belong to different entities, Part 1.5 requires the plan to identify each entity's

responsibilities. CIP-012-2 applies only to entities that own or operate a Control Center, and it exempts a Control Center sending data only about the generation or substation co-located with it. A distribution operations center that is not a Control Center under the Glossary is outside it.

4.3 Control Pathways

Direct control across the interface is usually narrow and tightly defined. Distribution operators generally cannot operate transmission equipment, and transmission operators generally cannot operate distribution equipment. Indirect influence is broader. Automated load shedding, Remedial Action Schemes, protection coordination and supervisory signals can all change what happens on the other side.

CIP-002-5.1a rates some of these paths explicitly. Under criterion 2.9, BES Cyber Systems associated with an SPS, RAS or automated switching System that operates BES Elements, and whose failure would cause IROL violations or reduce an IROL, are medium impact. Under criterion 2.10, the same applies to BES Cyber Systems associated with automatic UFLS or UVLS of 300 MW or more under a common control system. Where those systems reach into distribution substations, part of the distribution side is carrying medium impact obligations.

4.4 Visibility and Data Integrity

Visibility depends on more than whether data arrives. Operators need to know where it came from, how accurate it is and how old it is. An interface feed that delivers summarized or processed values can hide relationships between elements, and a compromise of upstream equipment can distort the picture in ways that are hard to spot.

The ERO's Event Analysis Process treats lost visibility as a reliability event in its own right. Category 1h covers loss of monitoring or control at a Control Center that degrades the entity's ability to make Real-time operating decisions for 30 continuous minutes or more, with loss of communications from SCADA remote terminal units given as an example. The process defines monitoring as the ability to accurately receive information and lists unacceptable state estimator or real-time contingency analysis solutions as an example, so bad data that degrades Real-time decisions for 30 continuous minutes can qualify. Plausible-looking corrupted data may never cross that threshold, which is why integrity deserves at least as much attention as availability.

Oversight does not audit how an entity designs its data exchange. It looks at whether the specified data was provided, whether the required plans exist and were implemented, and what happened when something failed. The design choices belong to the entities, and so does the risk that comes with them.

> **End-of-Chapter Summary**
>
> TOP-003-7, IRO-010-5 and CIP-012-2 put security duties on some interface data paths.

> **From the Field**
>
> Every data exchange across the T&D interface is a potential control pathway.

5 Shared Risk Without Shared Obligation

At the interface, the risk is shared and most of the regulatory responsibility is not. Getting that distinction right is what lets a program take interface risk seriously without inventing compliance obligations that don't exist.

5.1 What Shared Risk Means

Shared risk arises when a common factor or event can affect more than one system through operational, cyber or organizational dependencies. It exists even where BES and non-BES systems are cleanly separated on paper and subject to different rules. Cyber risk does not respect those separations. Trusted links, shared infrastructure and coordinated operating practices all give a malicious event a way across.

5.2 Where the Obligation Stops

The federal obligation is bounded by statute and by applicability sections. The ERO's authority covers only the bulk-power system. Each standard applies to the functional entities and facilities it lists, and an entity's participation in a shared system does not make it subject to a standard that doesn't list it. That is a deliberate choice. Mandatory requirements reach the systems needed for reliable operation of the bulk system, because tying obligation to any system that could propagate risk would undermine the clarity and enforceability of the standards.

In practice, a cyber event on a non-BES system is not, by itself, addressed by the BES standards. A distribution utility that holds no qualifying registration is not accountable to NERC for its effects on BES operations. The registered entity remains accountable for its own reliability obligations, wherever the risk came from.

5.3 Where the Standards Do Reach Across

"No shared obligation" is a simplification, and the original edition of this reference overstated it. The standards do allocate duties across the seam in several places:

- **Data specifications.** TOP-003-7 R5 and IRO-010-5 R3 obligate Distribution Providers that receive a data specification to satisfy it, including the agreed secure transfer method.
- **Control Center communications.** CIP-012-2 Part 1.5 requires entities with linked Control Centers to identify each party's responsibilities for protecting the data in transit.
- **Protection and restoration.** CIP-002-5.1a brings a Distribution Provider's qualifying load shedding, RAS, transmission protection and Cranking Path systems into CIP scope.

Outside those places, the obligation stays with each side, and the entity on the regulated side carries the boundary controls alone. Under CIP-003-9 Attachment 1 Section 3.1, for example,

the owner of an asset containing low impact BES Cyber Systems must permit only necessary inbound and outbound electronic access for routable communications crossing the asset boundary. Where that traffic originates is irrelevant to the obligation.

5.4 Closing the Gap Without Inventing Obligations

Two errors are common. The first imposes identical controls on every interfacing system so that no one has to coordinate. That spreads effort evenly instead of where the risk is, and it blurs who is accountable for what. The second treats any system outside scope as unimportant, which hides real vulnerabilities behind a correct scope determination.

What works, in my view, is awareness plus written allocation. Know the dependencies. Put them in the data specification, the interconnection or operating agreement, the CIP-012 plan and the incident response contacts. Where no rule assigns a duty, assign it by agreement. Reliability governance rests on well-defined boundaries, a clear division of responsibility and informed oversight, not on equal treatment of every device and system.

End-of-Chapter Summary

Cybersecurity reliability at the interface is a matter of shared risk and, mostly, separate regulatory responsibility. The standards apply only within their defined scope, but they do assign some cross-boundary duties through data specifications, CIP-012 and CIP-002's Distribution Provider provisions. The rest has to be handled by awareness, agreement and each entity's own program.

From the Field

The shared risk is real; most of the shared accountability is not codified.

6 Cybersecurity Threat Propagation Across System Boundaries

Cyber threats are not bounded by FERC jurisdiction or by functional registration. To assess risk at the interface, a program has to understand how a compromise on one side can reach the other.

6.1 How Compromise Propagates

Propagation pathways can exist whether or not the two systems are physically or logically separated, and whether or not they sit under different managers or regulators. Four are common at the interface.

- **Shared infrastructure.** Communication links carrying BES and non-BES operational, monitoring or supervisory traffic can spread an incident across system layers.
- **Trusted data exchange.** A Transmission Operator using distribution data for situational awareness, or a distribution utility using transmission data for restoration, will act on what it receives. If an attacker corrupts the data, operators may follow normal procedure on bad information without seeing anything wrong in their own systems.
- **Remote access.** Any path that lets a person reach across the boundary for operations support, maintenance or monitoring can carry an incident with it. Controls that comply with the standards still leave the access relationship in place.
- **Shared services and third parties.** A common data center, identity service or Security Information and Event Management platform can carry a compromise past segmentation that otherwise looks sound.

6.2 What the Standards Require on Those Paths

The CIP standards address several of these paths for in-scope systems.

Path	Requirement in force
Interactive Remote Access to high impact, and medium impact with External Routable Connectivity	CIP-005-7 R2: use an Intermediate System, encrypt to the Intermediate System, and require multi-factor authentication for every session
Vendor remote access to the same systems	CIP-005-7 R2.4 and R2.5: methods to determine active vendor sessions and to disable them

Path	Requirement in force
Vendor remote access to low impact assets	CIP-003-9 Attachment 1 Section 6 (effective April 1, 2026): methods to determine and disable vendor electronic remote access, and to detect known or suspected malicious communications
Routable access across a low impact asset boundary	CIP-003-9 Attachment 1 Section 3.1: permit only necessary inbound and outbound access
Vendor products and services	CIP-013-2: supply chain risk management plans for high and medium impact BES Cyber Systems and their associated EACMS and PACS

Interactive Remote Access excludes system-to-system process communications, so automated data exchange falls to the boundary controls and, between Control Centers, CIP-012-2, not CIP-005-7 R2.1 to R2.3. Vendor system-to-system remote access stays under R2.4 and R2.5.

6.3 A Documented Case: Ukraine, December 2015

The clearest public example of an attack through distribution systems remains the December 23, 2015 attack on Ukrainian distribution companies. The SANS ICS and E-ISAC analysis published March 18, 2016 describes how attackers gained access through spear phishing and BlackEnergy 3 malware, harvested credentials, and used VPN connections to enter the industrial control network. They then used the companies' own remote access tools and control systems to open breakers. Three distribution companies were affected and about 225,000 customers lost power for several hours. The attackers also loaded malicious firmware onto serial-to-Ethernet devices at substations, wiped systems with KillDisk, and flooded at least one customer call center.

The lesson for this chapter is the path, not the outcome. Every step ran through a trusted connection that was working as designed.

6.4 Potential Is Not Outcome

The existence of a path does not mean an event will travel it or cause harm. Countermeasures, protections and operating procedures often stop or contain it. The potential still belongs in the risk assessment and in planning. Event analysis looks back at what happened and why. It does not expand compliance scope, but it shows where awareness and preparation fell short.

> **End-of-Chapter Summary**
>
> Threats cross the boundary on shared paths; oversight answers with in-scope controls.

> **From the Field**
>
> The framework judges the in-scope controls, not where the attack began.

7 Critical Infrastructure Protection Context at the Interface

CIP is the main source of mandatory cybersecurity controls at the interface. Knowing exactly what it covers there, and what it does not, keeps a program from both under-scoping and over-reaching.

7.1 What CIP Covers at the Interface

CIP-002-5.1a applies to Balancing Authorities, qualifying Distribution Providers, Generator Operators, Generator Owners, Interchange Coordinators or Interchange Authorities, Reliability Coordinators, Transmission Operators and Transmission Owners. For each, the R1 process must consider six asset types, and the low impact list in Attachment 1 Section 3 tracks them:

1. Control Centers and backup Control Centers;
2. transmission stations and substations;
3. generation resources;
4. systems and facilities critical to system restoration, including Blackstart Resources, Cranking Paths and initial switching requirements;
5. Special Protection Systems that support reliable operation of the BES; and
6. for Distribution Providers, the Protection Systems specified in Section 4.2.1.

At a shared substation, the transmission side is an asset the Transmission Owner must evaluate. Its BES Cyber Systems are low impact unless a medium or high criterion applies. The distribution equipment in the same yard is outside CIP unless it belongs to one of the Distribution Provider categories in Chapter 2.

7.2 Low Impact Controls at Substations

Most interface substations hold low impact BES Cyber Systems, if any. Their controls come from CIP-003-9, effective April 1, 2026, which requires a documented plan covering cyber security awareness, physical security controls, electronic access controls, incident response, transient cyber asset and removable media malware mitigation, and vendor electronic remote access. Section 3, electronic access, is the interface control: it governs routable communications between a low impact BES Cyber System and Cyber Assets outside the asset. It does not apply to time-sensitive protection or control communications between intelligent electronic devices, such as IEC TR-61850-90-5 R-GOOSE.

FERC Order No. 918 (Docket No. RM25-8-000, March 19, 2026) approved CIP-003-11, which adds further low impact controls. NERC lists it as effective July 1, 2029.

7.3 Medium and High Impact at the Interface

Where a criterion applies, the controls deepen. A medium impact BES Cyber System with External Routable Connectivity sits inside an Electronic Security Perimeter, with routable traffic passing through an identified Electronic Access Point under CIP-005-7. Remote access goes through an Intermediate System with multi-factor authentication. Incident response under CIP-008-6 includes notifying the E-ISAC and, for U.S. entities, the National Cybersecurity and Communications Integration Center or its successor, within one hour of determining a Reportable Cyber Security Incident.

Interface element	CIP treatment
Transmission side of a shared substation	Asset evaluated under CIP-002; low impact unless a criterion applies
Distribution equipment in the same substation	Outside CIP unless a Distribution Provider category in Section 4.2.1 applies
Automatic UFLS or UVLS of 300 MW or more under a common control system	BES Cyber Systems associated with it are medium impact (criterion 2.10)
SPS, RAS or automated switching affecting IROLs	BES Cyber Systems associated with it are medium impact (criterion 2.9)
Communication networks and data links between discrete ESPs	Exempt from CIP-002 (Section 4.2.3.2)
RTA and Real-time monitoring data between Control Centers	CIP-012-2 plan

Interface element	CIP treatment
Distribution operations center not meeting the Control Center definition	Outside CIP

7.4 What CIP Does Not Do

CIP does not prohibit communication between BES and non-BES systems, and it does not require identical controls on both sides. It sets mandatory controls for in-scope systems and leaves the remaining risk to the entity's own program. Those controls reduce the chance that a compromise affects reliable operation. They do not try to eliminate threats on networks outside scope.

CIP oversight at the interface asks whether the entity identified its in-scope systems correctly and implemented the required controls. It does not evaluate the security of systems the entity correctly placed out of scope, except where their interaction with in-scope systems bears on a CIP requirement. Compliance is scoped and enforceable. Awareness of cybersecurity reliability has to be broader and risk-informed.

End-of-Chapter Summary

The CIP standards set scoped, impact-based requirements for the cyber systems that support BES functions. At the interface, the criteria in the standards decide what is in scope, not connectivity alone. The standards keep clear boundaries between regulated and unregulated systems and leave the shared risk to informed program decisions.

8 Functional Responsibility and Accountability at BES and Non-BES Boundaries

The NERC framework organizes obligations by function. That principle holds for cybersecurity at the interface, even as technical boundaries get harder to draw.

8.1 Function, Not Ownership

Requirements attach to the functions an entity registers for, not to who owns an asset, how a system is designed or how tightly it is interconnected. Many parties connect to T&D equipment to exchange data and coordinate restoration. Each is accountable for the reliability obligations of the functions it registered, for the portion of the system it controls. The Distribution Provider definition shows how literal this is: a Transmission Owner that serves end-use customers at transmission voltage is also the Distribution Provider for them.

For cybersecurity, an entity is accountable for the in-scope systems that support its registered functions. It is not responsible for securing every system connected to or influenced by those systems.

8.2 Transmission-Side Accountability

Transmission entities have to perform their functions in a way that keeps their control systems, communications and data networks working. That includes understanding their dependence on non-BES systems and shared services, even where the dependency itself is unregulated. TOP-003-7 makes that concrete for data: the Transmission Operator decides what non-BES data it needs, from whom, and by what secure method.

8.3 Distribution-Side Accountability

Most distribution entities are not registered for bulk system functions. Their cybersecurity obligations come from their own policies, state regulation and voluntary practices, not from NERC. DOE's February 22, 2024 announcement of the NARUC cybersecurity baselines put it plainly: regulatory oversight of electric distribution systems and distributed energy resources occurs at the state level. NARUC's *Cybersecurity Baselines for Electric Distribution Systems and DER*, funded by DOE's Office of Cybersecurity, Energy Security, and Emergency Response, is a resource for state commissions, distribution utilities and DER operators and aggregators in states that choose to adopt it.

The absence of federal oversight does not make the distribution side less important. It means the controls there rest on a different authority.

8.4 Third Parties Do Not Take the Obligation

Outsourcing a function does not transfer the obligation. The Glossary definition of Real-time Assessment allows the assessment to be provided through third-party services, but the Transmission Operator still owns the requirement to perform it. CIP-013-2 exists because vendors, data centers and managed services sit inside the risk of high and medium impact systems while the registered entity keeps the compliance obligation.

8.5 Accountability When One Attack Hits Several Systems

When a single attack affects multiple systems at the interface, accountability looks at whether each organization acted appropriately within its own scope. It does not try to apportion blame across organizational boundaries. Response coordination works when responsibilities are assigned in advance and contacts are already established. Uncertainty about who does what costs time, and time matters during an incident.

Reliable cybersecurity does not require any one party to control everything. It requires each party to perform its assigned role, with clear boundaries of authority and practiced coordination on the cross-cutting work.

End-of-Chapter Summary

Functional responsibility defines cybersecurity accountability at the interface. An entity stays accountable for the in-scope systems that support its registered functions, even when the risk is shared across boundaries. That keeps accountability clear and supports operational coordination. It also adds no regulatory burden beyond what the standards already impose.

From the Field

NERC standards are reliability standards with cybersecurity components. They aren't cybersecurity standards. The distinction matters when an entity tries to use compliance as a security baseline.

The standards establish a floor. The threat environment is above the floor. A program built only to the floor is a program operating below the threat baseline.

9 Oversight, Compliance Monitoring, and Enforcement Considerations

Oversight at the interface runs through the same Compliance Monitoring and Enforcement Program as everything else. What changes is how the scope questions show up.

9.1 How Monitoring Works

Appendix 4C of the NERC Rules of Procedure (effective May 19, 2022) sets the monitoring processes: Compliance Audits, Self-Certifications, Spot Checks, Compliance Investigations, Self-Reports, Self-Logging, Periodic Data Submittals and Complaints. Audits are risk-based. The Compliance Enforcement Authority tailors audit scope to the Reliability Standards identified through NERC-approved risk-based processes, including Inherent Risk Assessments and internal controls, and may include applicable standards whether or not they appear in the annual CMEP Implementation Plan.

For transmission and distribution entities, monitoring focuses on the BES Cyber Systems, communications and control activities within scope. It does not require a full evaluation of non-BES systems in the operational environment. Audits, spot checks and investigations can still examine interface conditions where they bear on an applicable requirement.

9.2 What an Audit Team Looks at

At the interface, the questions tend to follow the requirements already described:

- Does the Transmission Operator have a dated, current data specification under TOP-003-7, distributed to the entities that hold the data, with a secure transfer method?
- Can the Distribution Provider show it satisfied the specification it received?
- For each asset containing low impact BES Cyber Systems, what routable communications cross the asset boundary, and what permits only the necessary ones under CIP-003-9 Attachment 1 Section 3.1?
- Is every medium impact BES Cyber System at the interface identified, including those associated with load shedding and RAS systems that reach into distribution substations?
- Where Control Centers exchange Real-time data, does the CIP-012-2 plan identify each entity's responsibilities?

Risk-based oversight can put more attention on complex, highly dependent interfaces without changing any applicability threshold.

9.3 Enforcement Follows the Requirement

Enforcement determinations rest on the language of the requirement and the evidence. A noncompliance finding requires a violated requirement that applies to the registered entity's functions and facilities. Conditions outside the BES, including problems on non-BES systems,

are not on their own a basis for enforcement. Mitigation is scoped the same way. Appendix 4C requires a Mitigation Plan to correct the noncompliance and prevent recurrence. It does not require the entity to fix systems outside its scope.

9.4 What the Enforcement Record Shows

NERC's ORCP and CMEP Annual Report, published February 11, 2026, lists CIP-010, CIP-007 and CIP-004 as the most frequently reported CIP noncompliance in 2025, all involving high volume and high frequency conduct. It identifies lacking or deficient policies and procedures as the leading root cause for those three. CIP-003 and CIP-005, the standards that govern boundary access, are also on the top-ten list. None of that is interface-specific. In my view, the interface is where boundary documentation tends to be thinnest.

Event reviews add a learning channel without expanding enforcement. Chapter 10 covers them. Compliance oversight keeps entities meeting the requirements that apply to them. Cybersecurity reliability at the interface also needs coordination and operating discipline that the requirements do not define.

End-of-Chapter Summary

Oversight of cybersecurity at the interface happens inside the existing monitoring and enforcement framework, on a risk basis and with due process. Shared risk can shape where monitoring focuses. Enforcement still rests on the applicable requirements and the entity's registered functions.

From the Field

Audit findings at the T&D interface tend to be subtle. At a low impact asset, CIP-003-9 Attachment 1 Section 3.1 turns on which routable communications cross the boundary, and in my view an undocumented connection is the hardest one to answer for.

A finding that traces to an unregulated system feeding a regulated system is still a finding against the regulated entity.

A program that maps data flows across the interface, in writing, has its answer ready when the audit team asks. A program that mapped only its CIP-scoped assets has to build that answer during the audit.

10 Disturbance Experience and Reliability Lessons Involving Interfaces

Events teach what the standards cannot. They show that reliability outcomes depend on how systems and people behave under stress, not only on whether each entity met its requirements.

10.1 How the ERO Learns From Events

The ERO Event Analysis Process, Version 5.0, effective January 1, 2024, is forensic. It focuses on near-term and real-time horizons, and its main objective is for the ERO and industry to learn from events and develop corrective actions to prevent recurrence. Events are categorized by impact, analyzed, and turned into lessons learned shared with industry.

Two category definitions bear on the interface. Category 1h, covered in Section 4.4, is one. Category 1e covers BES separation into an island of 100 MW to 999 MW, and it expressly excludes non-BES (distribution) level islanding. The process is built around BES impact, so a distribution-side event enters the record when it affects the BES or when the entity volunteers it.

10.2 A Lesson Learned: Firewall Firmware, 2019

NERC's September 2019 lesson learned, *Risks Posed by Firewall Firmware Vulnerabilities*, describes an entity with a low impact control center and multiple remote low impact generation sites. An attacker exploited a known vulnerability in the web interface of internet-facing perimeter firewalls, causing reboots over a 10-hour period. Each outage lasted less than five minutes and none affected generation. A firmware update that fixed the vulnerability had been released before the event.

The lessons NERC drew apply squarely at the interface: follow good patch and vulnerability management even at low impact assets, and restrict firewall rules to the minimum traffic needed. The perimeter device is where the two sides of any boundary meet, and it is only as good as its maintenance.

10.3 What Ukraine Showed About Restoration

The 2015 Ukrainian attack described in Chapter 6 also holds restoration lessons. With serial-to-Ethernet devices disabled by malicious firmware and systems wiped, the affected companies restored service through manual operations. A program that has never practiced restoring without SCADA visibility is assuming its control systems will be there when it needs them most.

10.4 Patterns at the Interface

The public record and the requirements point to recurring themes:

- Loss of visibility, degraded data or broken coordination can complicate response even when the primary BES control systems are untouched.
- Protection systems at the boundary, and the cyber systems that manage their settings and communications, can turn a local problem into a wider one.
- Human factors recur: unclear roles, slow information flow between transmission and distribution, and assumptions about who will act. Cyber disruption to communications makes all of them worse.

In my view, the biggest value of event analysis is that it looks at functional performance and coordination, not at who was classified as BES or non-BES. That reinforces the systems view of cybersecurity reliability without any new regulation.

End-of-Chapter Summary

Disturbance experience shows how cybersecurity and operational problems at the interface can affect BES reliability indirectly. Lessons learned focus on functional performance and shared risk rather than compliance status. Acting on them as a reliability matter strengthens programs without waiting for regulatory action.

From the Field

"It's distribution, so CIP doesn't apply" is correct on scope and wrong on risk. Scope and risk are not the same thing.

"We segmented the network" is necessary but doesn't end the conversation. Segmentation is a control, not a guarantee. In my view, a program should be able to show how its segmentation was validated, even where no requirement asks.

"The transmission and distribution sides have different security teams" is common. In my view, that split is a seam an adversary can use.

11 Common Misconceptions About Transmission and Distribution Cybersecurity Risk

The interface is widely misunderstood because technology, regulation and operations all meet there. These are common misconceptions about it, with the correction for each.

11.1 "Cyber risk at the interface is a compliance problem"

Managing risk at the interface does not mean someone is out of compliance. Cyber risk on non-BES systems is not a failure of the standards. The standards set mandatory requirements within a defined scope and leave the rest to each entity's program.

11.2 "If it connects to the BES, CIP covers it"

Connection is not the test. CIP-002 applies through defined functional entities, assets and impact criteria. Section 4.2.3.4 exempts every Distribution Provider system outside the four listed categories, and Section 4.2.3.2 exempts communication networks and data links between discrete ESPs. Pulling every connected system into scope muddies the definitions the standards depend on.

11.3 "Distribution is never in CIP scope"

The reverse error is just as common. A Distribution Provider that owns a qualifying UFLS or UVLS system, a RAS, a transmission Protection System or Cranking Path Elements has CIP obligations for those systems, and under criteria 2.9 and 2.10 the BES Cyber Systems associated with those systems can be medium impact.

11.4 "The transmission side has to secure the distribution side"

Function-based responsibility means the distribution owner and operator remains responsible for the systems it manages. A Transmission Owner or Operator has to manage its own systems and its dependencies, including the boundary controls on its side. It does not have to run anyone else's cybersecurity program.

11.5 "Auditors audit the non-BES side too"

Audits test defined requirements for in-scope systems. Interfaces may appear in an audit for context, but there is no compliance audit of non-BES systems unless they fall under an applicable requirement.

11.6 "Compliance means security," and "guidance means requirement"

A system can be fully compliant and still face reliability problems from cyber issues at interface points where dependent systems are not fully trusted or understood. Guidance documents, lessons learned and voluntary baselines such as NARUC's are valuable warnings about risk. They are advisory. They are not Reliability Standards.

11.7 "Eliminate the dependencies and the risk goes away"

It can't be done, and it isn't the goal. The grid runs on information sharing, coordination and common infrastructure. Reliability and resilience come from understanding and managing the dependencies that can't be removed.

End-of-Chapter Summary

Misconceptions at the interface usually come down to three: that connectivity creates compliance obligations, that every interfacing system needs compliance coverage, and that compliance equals resilience. Correcting them keeps function-based responsibility intact and grounds each utility's awareness of shared risk in how the framework actually works.

12 Evolving Interfaces, Emerging Technologies, and Future Considerations

The interface keeps changing with technology, operating practice and system configuration. The principles underneath it do not. This chapter covers the changes already on the books and how I think programs should read them.

12.1 Distributed Resources and Automation

Distributed energy resources, advanced distribution management systems and automated control are increasing communication within distribution networks and between distribution and transmission. FERC Order No. 2222 (Docket No. RM18-9-000, issued September 17, 2020) requires RTOs and ISOs to let distributed energy resource aggregations participate in their markets, with a minimum aggregation size not to exceed 100 kW. Aggregation adds another layer of communication and control between small resources and bulk system operations. These developments can improve reliability, and they add cyber risk that the risk assessment has to account for.

Digital systems have also changed the speed and volume of transactions across the boundary. Better visibility improves situational awareness, and it makes the system more sensitive to failures of data integrity or availability.

12.2 CIP Changes Already Approved

Date	Change
April 1, 2026	CIP-003-9 in effect, adding vendor electronic remote access controls for low impact assets
July 1, 2026	CIP-012-2 in effect: plans must address unauthorized disclosure, unauthorized modification and loss of availability of Real-time data between Control Centers
October 1, 2026	TOP-003-7 in effect (data specifications including non-BES data)
July 1, 2028	CIP-002-8 takes effect: the revised Control Center definition reaches a Transmission Owner that can control transmission Facilities at two or more locations using SCADA, and criterion 2.12 uses a weighted value threshold of 6,000 with an exclusion for local systems that mainly serve load (FERC Docket No. RD25-8-000, March 19, 2026). CIP-002-7 is retired immediately before it. The virtualization revisions across the CIP family take effect the same day (FERC Order No. 919, Docket No. RM24-8-000, issued March 19, 2026)
October 1, 2028	CIP-014-4 (physical security) in effect; CIP-015-1 internal network security monitoring for high impact and medium impact with External Routable Connectivity

Date	Change
July 1, 2029	CIP-003-11 adds further low impact controls (Order No. 918)
October 1, 2029	CIP-015-2 extends INSM to associated EACMS and PACS (and supporting Shared Cyber Infrastructure); traffic to or from low impact systems and between discrete ESPs stays out of scope

The INSM standards trace to FERC Order No. 887 (Docket No. RM22-3-000, issued January 19, 2023), which directed new or modified standards for internal network security monitoring and a NERC study of low impact systems and medium impact systems without External Routable Connectivity. FERC approved CIP-015-1 in Order No. 907 (Docket No. RM24-7-000, June 26, 2025). The CIP-002-8 change matters most for this paper: some Transmission Owner SCADA facilities that sit right at the interface will carry Control Center obligations for the first time.

12.3 Distribution Baselines at the State Level

On the distribution side, the movement is through the states. NARUC's February 2024 baselines, built from CISA's Cross-Sector Cybersecurity Performance Goals and tailored to distribution systems and DER, give states a common starting point. They cover topics such as asset inventory, network segmentation, phishing-resistant multi-factor authentication and documentation of network topology. Their reach depends on whether each state adopts them.

12.4 Organizational Change

Shared services, centralized security operations centers and cloud services are changing the scope of IT and OT work, and the boundaries staff are authorized to cross, without changing the underlying obligations. Governance, clear roles and a defined interface matter more as digital connections blur the physical lines between organizations.

12.5 What Stays the Same

In my view, the evolving interface does not argue for expanding regulatory scope across transmission and distribution. It argues for checking whether current requirements and voluntary risk reduction actually address the risks being identified. The interfaces of the future will be part of larger systems with larger attack surfaces and a greater need for coordinated recovery. The framework handles that by tying responsibility to function and outcome rather than to technology.

The distinction between shared risk and shared obligation should hold as complexity rises. Event analysis, technical studies and voluntary information sharing will keep improving understanding of interface risk without premature or rigid regulatory change.

> **End-of-Chapter Summary**
>
> The interface is changing faster than the principles under it. Approved CIP revisions through 2029 reach further into it, and distribution baselines are moving through the states.

Glossary

Term	Meaning in this paper
Bulk Electric System (BES)	NERC Glossary term: unless modified by the listed inclusions and exclusions, 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.
Critical Infrastructure Protection (CIP) Standards	The NERC Reliability Standards, CIP-002 through CIP-015, that set cyber and physical security requirements for systems relied on for reliable operation of the BES.
Cybersecurity Reliability	Working term used in this reference: the ability of cyber systems and supporting processes to sustain or restore reliable operation of the electric system in the presence of cyber threats, vulnerabilities or disruptions.
Distribution Provider	NERC Glossary term: the entity that provides and operates the "wires" between the transmission system and the end-use customer, at any voltage. Registered only when it meets the criteria in Rules of Procedure Appendix 5B.
Distribution System	Working term: facilities and systems that deliver energy from transmission lines or distribution substations to the point of use and are not part of the BES.
External Routable Connectivity	NERC Glossary term: the ability to access a BES Cyber System from a Cyber Asset outside its associated Electronic Security Perimeter via a bi-directional routable protocol connection.
Functional Responsibility	The principle that reliability obligations attach to the functions an entity is registered to perform, regardless of who owns an asset or how a system is built.
Interactive Remote Access	NERC Glossary term: user-initiated access by a person using a remote access client or other remote access technology over a routable protocol, from outside the entity's ESPs. It does not include system-to-system process communications.
Interface	Working term: the point where transmission and distribution systems connect physically, logically or operationally, allowing power, data or control to pass from one to the other.
Non-BES System	Any facility or cyber system that does not meet the BES definition or the applicability criteria of the relevant standard.
Operational Interdependence	The condition in which the operation of one system affects others through coordinated activity, information exchange or shared resources.
Oversight	The processes by which NERC, the Regional Entities and FERC monitor, audit and enforce compliance with Reliability Standards and assess reliability risk.

Term	Meaning in this paper
Real-time Assessment	NERC Glossary term: an evaluation of system conditions using Real-time data to assess existing and potential operating conditions. It may be provided through internal systems or through third-party services.
Risk-Based Oversight	An approach to compliance monitoring and enforcement that sets scope and priority by the reliability risk an entity and its noncompliance pose, using tools such as Inherent Risk Assessments.
Shared Risk	The condition in which an entity's reliability outcomes can be affected by systems or entities outside its control or outside its compliance scope.
Transmission System	Working term: the high-voltage facilities and systems that move bulk electric energy over long distances.

The NERC Glossary of Terms governs any term it defines. Working terms here are for explanation only and are not a basis for any compliance determination.

How Energy Compliance Can Help

The interface is a scoping problem first and a security problem second. 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, and data request strategy; registration and applicability analysis, including Distribution Provider and BES exception questions; 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 interface obligations, such as TOP-003 data specifications, organized and ready. 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 operations-data path RenewOps depends on is an interface path worth mapping.

Start with the data that crosses your interface. If you can't list it, 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

- Federal Power Act Section 215, Electric Reliability, 16 U.S.C. 824o. https://govinfo.gov/link/uscode/16/824o
- North American Electric Reliability Corporation (NERC), Glossary of Terms Used in NERC Reliability Standards. https://www.nerc.com/glossary-of-terms
- NERC, Rules of Procedure, Appendix 5B, Statement of Compliance Registry Criteria. https://www.nerc.com/globalassets/who-we-are/rules-of-procedure/appendix-5b.pdf
- NERC, Rules of Procedure, Appendix 5C, Procedure for Requesting and Receiving an Exception from the Application of the NERC Definition of Bulk Electric System. https://www.nerc.com/globalassets/who-we-are/rules-of-procedure/appendix-5c.pdf
- NERC, Rules of Procedure, Appendix 4C, Compliance Monitoring and Enforcement Program. https://www.nerc.com/globalassets/who-we-are/rules-of-procedure/appendix-4c.pdf
- NERC, Reliability Standard CIP-002-5.1a, Cyber Security: BES Cyber System Categorization. https://www.nerc.com/globalassets/standards/reliability-standards/cip/cip-002-5.1a.pdf
- NERC, Reliability Standard CIP-003-9, Cyber Security: Security Management Controls. https://www.nerc.com/globalassets/standards/reliability-standards/cip/cip-003-9.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-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-012-2, Cyber Security: Communications between Control Centers. 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. 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, Reliability Standard TOP-003-7, Transmission Operator and Balancing Authority Data and Information Specification and Collection. https://www.nerc.com/globalassets/standards/reliability-standards/top/top-003-7.pdf
- NERC, Reliability Standard IRO-010-5, Reliability Coordinator Data and Information Specification and Collection. https://www.nerc.com/globalassets/standards/reliability-standards/iro/iro-010-5.pdf
- NERC, ERO Event Analysis Process, Version 5.0. https://www.nerc.com/globalassets/programs/event-analysis/ero-event-analysis-process-documents/ero_eap_v5.0.pdf
- NERC, Lesson Learned, Risks Posed by Firewall Firmware Vulnerabilities. https://www.nerc.com/pa/rrm/ea/Lessons%20Learned%20Document%20Library/20190901_Risks_Posed_by_Firewall_Firmware_Vulnerabilities.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
- Federal Energy Regulatory Commission (FERC), Order No. 887, Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems, Docket No. RM22-3-000. https://www.govinfo.gov/content/pkg/FR-2023-02-09/pdf/2023-01453.pdf
- FERC, Order No. 907, Critical Infrastructure Protection Reliability Standard CIP-015-1, Docket No. RM24-7-000. https://www.govinfo.gov/content/pkg/FR-2025-07-02/html/2025-12309.htm
- FERC, Order No. 918, Critical Infrastructure Protection Reliability Standard CIP-003-11, Docket No. RM25-8-000. https://www.govinfo.gov/content/pkg/FR-2026-03-24/pdf/2026-05711.pdf
- FERC, Order Approving Reliability Standard CIP-002-8, Docket No. RD25-8-000. https://www.govinfo.gov/content/pkg/FR-2026-03-24/pdf/2026-05715.pdf
- FERC, Order No. 919, Virtualization Reliability Standards, Docket No. RM24-8-000, 91 FR 13957 (March 24, 2026). https://www.govinfo.gov/content/pkg/FR-2026-03-24/pdf/2026-05716.pdf
- FERC, Order No. 2222, Participation of Distributed Energy Resource Aggregations in Markets Operated by Regional Transmission Organizations and Independent System Operators, Docket No. RM18-9-000. https://www.ferc.gov/media/ferc-order-no-2222-fact-sheet
- National Association of Regulatory Utility Commissioners (NARUC), Cybersecurity Baselines for Electric Distribution Systems and DER (February 2024). https://www.energy.gov/sites/default/files/2025-01/NARUC_Cybersecurity-Baselines-Report%201.pdf
- U.S. Department of Energy, CESER, announcement of the NARUC cybersecurity baselines (February 22, 2024). https://www.energy.gov/node/4838217
- SANS Industrial Control Systems and Electricity Information Sharing and Analysis Center (E-ISAC), Analysis of the Cyber Attack on the Ukrainian Power Grid, Defense Use Case. https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf

© Energy Compliance, Inc. · EC-WP-205 · October 2026