CYBERSECURITY · CIP SERIES · EC-WP-206

Remote Operations & Control Centers

Remote and virtual control center compliance in the post-COVID, AI age.

Remote and virtual control center operations spread during COVID-19 and never went back. The CIP scope did not change, but the way an entity has to demonstrate compliance did. This reference explains why function, not location, sets the obligation, and what the standards in force in October 2026 require for remote access, backup functionality, and operating communications.

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

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

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

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

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

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

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

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

Rob Smith

Founder and Principal, Energy Compliance, Inc.

Executive Summary

Remote and virtual control center operations spread fast during COVID-19 and never went back. The CIP scope did not change. What changed is where the operator sits, what the operator depends on to see the system, and how much of the control path now runs over networks the entity does not physically walk. If your operator can change a setpoint from a kitchen table, the access path into that control system is in CIP scope, and the network carrying it is part of your reliability architecture.

The NERC framework handles this better than most people expect, because it was built on functions rather than buildings. A Control Center under the NERC Glossary is defined by the operating personnel and the reliability tasks they perform, not by an address. That same design means there is no remote-operations exception anywhere in the standards. This reference walks through what that means in practice:

- **A control center is wherever the function is performed.** The registered function defines the obligation, not the address. CIP-002 rates the BES Cyber Systems at Control Centers and backup Control Centers by the functional obligations those centers serve (Chapters 2 and 6).
- **Network architecture is now reliability architecture.** Designed correctly, the firewall replaces the wall. Designed casually, it does not (Chapter 6).
- **Remote operation shifts the failure modes.** Network paths, video feeds and authentication services become single points of failure, and the program has to track them alongside the old ones (Chapter 5).
- **CIP-005 expectations do not relax for remote operators.** The Interactive Remote Access requirements in CIP-005-7 Part 2 (Intermediate System, encryption, multi-factor authentication) govern exactly this use case (Chapter 7).
- **Backup capability is functional, not physical.** EOP-008-2 requires Reliability Coordinators, Balancing Authorities, and Transmission Operators to plan a transition to backup functionality of two hours or less and to test it every year (Chapters 4 and 10).
- **The evidence is where remote programs break.** In my view, three areas deserve a self-audit before any Regional Entity asks: a complete asset and access-path inventory, Interactive Remote Access logging, and the physical security position for remote workstations (Chapter 9).
- **The rules keep moving.** CIP-012-2 took effect July 1, 2026. The virtualization revisions to the CIP family and CIP-002-8, with a revised Control Center definition, take effect July 1, 2028 (Chapter 12).

1 Evolution of Remote Operations and Control Centers

This reference addresses remote and virtual control center operations in the context of the NERC Reliability Standards, including the Critical Infrastructure Protection (CIP) standards, and the oversight that goes with them. Keep one distinction in view throughout: Reliability Standards are mandatory and enforceable, while guidelines, reference documents, and lessons learned are voluntary. Where this reference cites a guideline, it says so.

1.1 From Hardwired Rooms to Networked Operations

Control centers have always been central to real-time operation of the bulk electric system. Say "control center" and most people picture a large physical building, with system operators, shift supervisors, and support staff seated together in front of a wall of displays. That picture is accurate for some entities. For many others it is a memory.

Early control centers reflected the constraints of analog communications and local control. Dedicated voice circuits, hardwired telemetry, and on-site automation connected the operator to transmission and generation equipment. Proximity to the equipment, and to the people who maintained it, was built into the practices and assumptions of the day.

Decades of digital control systems, supervisory control and data acquisition (SCADA), and wide-area communications changed that. Operators can now manage facilities from much greater distances with more visibility and finer detail than the old boards ever gave them. With redundant communications paths, the operator is no longer tied to a single room.

1.2 Backup and Distributed Control Were Always Functional

Business pressures pushed in the same direction. Work that once required on-site staff at far-flung assets was centralized into shared operations centers to save cost. At the same time, reliability practice focused more on making sure that no single event, whether caused by people or by weather, could take down the ability to operate the system.

That is why "remote operations" has never meant only operations in remote places. Backup control centers, hot-standby facilities, and shared control arrangements were designed in to improve reliability. Availability was treated as a property of the function, not of a building. EOP-008-2, Loss of Control Center Functionality, codifies that thinking today: it speaks of "backup functionality," which a Balancing Authority or Transmission Operator may provide through a facility or through contracted services.

1.3 What COVID-19 Changed

The pandemic turned remote operation from a contingency into a routine. On March 18, 2020, FERC and NERC issued joint guidance so that operators of the bulk electric system could focus their resources on keeping the lights on. The guidance treated pandemic effects as an acceptable basis for PER-003-2 operator certification noncompliance from March 1 through December 31, 2020, provided entities notified their Regional Entity and Reliability Coordinator when they used non-certified operators. It also postponed on-site audits, certifications, and other on-site activities until at least July 31, 2020.

Notice what the guidance did not do. It did not suspend the CIP standards, and it did not create a separate rule set for operators working from home or from split shifts at backup sites. The functional obligations stayed where they were. Entities had to meet them from new places.

1.4 New Dependencies, Same Accountabilities

Virtualization, remote access, and distributed infrastructure have since pushed the boundary further. Control tasks are no longer confined to an on-site control room. They can be performed from a regional office, a backup facility, a mobile unit, or a home office.

The NERC framework absorbs this well because it assigns responsibility by function. As control center structures changed, from local plant control rooms to fleet-wide operations centers monitoring dozens of sites, the functional definitions did not need rewriting. That remains one of the framework's real strengths.

But remote and virtual operation does introduce new dependencies and new sources of risk: heavier reliance on communication systems, more exposure to cyber threats, and a different relationship between the operator, the team, and the equipment. None of these changes the accountability. All of them change how the accountability is discharged, and how the entity proves it.

Chapter Summary

Control centers began as large, fixed facilities. Technology, business consolidation, and emergency preparedness produced backup, distributed, and virtual arrangements, and COVID-19 made remote operation routine. The NERC framework still describes obligations in functional terms. The new dependencies have to be managed inside the existing reliability and security requirements, not around them.

From the Field

Remote control is not new. What is new is that remote control is now normal, and most of the standards were written when it was not. The control center moved. The operators moved with it. The reliability obligations did not move; they followed the function, wherever the function was performed.

2 Control Center Functions and Reliability Responsibility

A control center is a place that provides the resources to perform reliability tasks. Whether those tasks are performed from a head office, a field office, or a home office, the tasks are the ones the Reliability Standards describe. Getting this right, and not letting the location of the work cloud the analysis, is the first step in every remote operations program.

2.1 What NERC Means by "Control Center"

The NERC Glossary of Terms defines a Control Center as one or more facilities hosting operating personnel that monitor and control the Bulk Electric System in real time to perform the reliability tasks, including their associated data centers, of a Reliability Coordinator, a Balancing Authority, a Transmission Operator for transmission Facilities at two or more locations, or a Generator Operator for generation Facilities at two or more locations.

Three things in that definition matter for remote operations:

- **It turns on people and tasks.** The trigger is operating personnel performing real-time monitoring and control. The definition does not require a dedicated building.
- **It includes associated data centers.** A virtualized platform hosted somewhere else is part of the Control Center it serves.
- **It reaches multi-site Generator Operators.** A renewable or storage operations center that monitors and controls generation Facilities at two or more locations meets the definition.

A revised definition approved by FERC with CIP-002-8 (Docket No. RD25-8-000, March 19, 2026) adds one or more facilities of a Transmission Owner that can control transmission Facilities at two or more locations in real time using SCADA, including associated data centers and excluding field Cyber Assets used for telemetry. NERC lists that definition as subject to future enforcement on July 1, 2028.

2.2 Responsibility Follows the Registered Function

NERC assigns responsibility to registered entities by function, not by physical facility. Typical control center work includes tracking real-time system conditions, carrying out Operating Instructions, coordinating with neighboring systems, and responding to emergencies. The reliability effect of those actions depends on the scope of authority and the quality of situational awareness. It does not depend on where the operator sits.

So a Transmission Operator or Balancing Authority whose operators work remotely, or whose platforms are virtualized, carries exactly the same obligations under the standards that apply to it. The entity performing the function keeps every responsibility that comes with it.

The same logic applies to backup arrangements. Authority to operate may be transferred to a backup Control Center or an alternate location for defined conditions and periods, and the reliability requirements travel with it. EOP-008-2 R4 requires a Balancing Authority's or Transmission Operator's backup functionality to include monitoring, control, logging, and alarming sufficient for maintaining compliance with all Reliability Standards that apply to its primary control center functionality.

2.3 Authority and Interdependence Do Not Change with Distance

Authority is central to control center responsibility. Operating personnel need clear authority to act within their Operating Procedures and to carry out Reliability Coordinator directives. That need does not shrink when the operator is remote. If anything it grows, because the remote setting removes the informal cues that settle questions in a shared room. Clear command authority and written escalation paths fill that gap.

Control center functions are also tightly linked. When a Balancing Authority moves generation to correct an imbalance, transmission loading changes. When a Transmission Operator acts to manage a local constraint, flows shift elsewhere. Reliability Coordinator actions span a wide area. Remote operation does not remove any of these links, and in some arrangements it makes coordination harder.

2.4 Human Factors Still Decide Outcomes

Operator judgment, workload management, and communication remain decisive. A remote environment changes how those activities happen. It does not change the need for proven operating practices and training.

From a functional view, even when the physical structure of a control center changes, the basic elements stay the same: authority, coordination, situational awareness, and accountability. Reliability is the result of identified functions being performed well, not of the design or location of the room.

Chapter Summary

A Control Center is defined by its function, not its location. The registered entity performing operating functions keeps its responsibility for reliability whether control is exercised from a primary room, a backup site, or a virtual platform. Authority, coordination, and situational awareness remain the elements that matter.

From the Field

Every remote program needs a written position on whether the operator's location is itself part of a Control Center. The standards contain no remote-operations exception, and the operational evidence has to show the same capability the primary room shows.

3 Situational Awareness and Communications Dependency

Situational awareness is basic to reliable operation. Operating personnel need a timely, accurate, and complete picture of system conditions to spot developing problems, respond to disturbances, and coordinate across the interconnected system. In remote and virtual control centers, that picture depends heavily on communications and data systems.

3.1 Data Availability and Integrity

Operators need a steady flow of information: telemetry, alarms, State Estimator results, and the analyses built on them. NERC defines a Real-time Assessment as an evaluation of system conditions using Real-time data to assess existing and potential post-Contingency operating conditions, and notes that it may be provided through internal systems or through third-party services. Each of those inputs travels further in a remote model, across more network segments and more access points.

If data arrives late, goes missing, or is distorted, the operator's picture degrades, and so does readiness to act. CIP-012-2, Communications between Control Centers, effective July 1, 2026, addresses part of this risk directly. It requires the entity to implement one or more documented plans to mitigate the risks of unauthorized disclosure, unauthorized modification, and loss of availability of Real-time Assessment and Real-time monitoring data while that data is transmitted between Control Centers. The plan must also identify methods to initiate recovery of the communication links. Where the Control Centers belong to different entities, the plan must identify each entity's responsibilities.

3.2 Interpersonal Communication and Its Backup

Voice coordination among operators, field crews, Reliability Coordinators, and neighboring Transmission Operators is needed every day and matters most in emergencies. Remote control centers typically use a mix of analog and digital voice paths, including IP telephony, with backup systems behind them. More components means more places to fail, which is why redundancy has to be engineered rather than assumed.

COM-001-3 sets the floor. Reliability Coordinators, Transmission Operators, and Balancing Authorities must have Interpersonal Communication capability with specified entities and must designate an Alternative Interpersonal Communication capability, which the Glossary defines as one that can substitute for day-to-day communication and does not use the same infrastructure. Requirement R9 requires those entities to test the alternative capability at least once each calendar month and, if a test fails, to initiate repair or designate a replacement within two hours. Requirement R12 requires Reliability Coordinators, Transmission Operators, Generator Operators, and Balancing Authorities to have internal Interpersonal Communication capabilities,

including between Control Centers within the same functional entity and between a Control Center and field personnel.

For remote operators, those requirements answer a practical question: if the home internet connection fails during an event, what is the alternative path, and does it share infrastructure with the primary one?

3.3 How Situational Awareness Is Lost

Loss of situational awareness takes many forms. Operators may miss a change in system state, misread an alarm, or not get information in time during an emergency. In remote settings the causes include network failures, cyberattacks on SCADA, data center outages, and misconfigured remote access.

The standards treat the most severe version as a reportable event. Under EOP-004-4, a Reliability Coordinator, Balancing Authority, or Transmission Operator must report a complete loss of monitoring or control capability at its staffed BES control center for 30 continuous minutes or more.

The situational awareness standards do not mandate a technology or an architecture. They set performance requirements for the communications, information flows, and coordination that situational awareness depends on. The entity's control environment, wherever it is, has to support those requirements.

3.4 The Operator Interface at a Distance

Remote operation can change how an operator interacts with the human-machine interface (HMI), alarms, and support tools. Screen size, the number of displays, alarm audibility, and the operator's ability to see what a colleague is looking at may all differ from the primary room. Communication between people in different places, and between people and distant equipment, also changes.

The existing reliability requirements still govern, and the communications and data systems behind remote operations belong to the reliability system that makes operating decisions possible.

> **Chapter Summary**
>
> In remote operations, situational awareness depends on communications and data systems. COM-001-3, CIP-012-2, and EOP-004-4 set the minimum expectations for keeping it intact.

> **From the Field**
>
> A remote operator depends on the network to see the system. Network problems become operating problems faster than in a physical control center, where the operator can walk down the hall. Communications redundancy is not a luxury for remote operations. It is the operating premise. Lose the link without a tested alternative and you lose the control.

4 Authority, Coordination, and Operating Boundaries

Reliability has to hold wherever control is exercised. When people, systems, and facilities are physically separated, clear definitions of authority and operating boundaries matter more, not less.

4.1 Where Authority Comes From

Authority in a control center means the ability to direct actions, issue instructions, and obtain a response from systems and equipment for the functions assigned to its personnel. For Transmission Operators, Balancing Authorities, and Reliability Coordinators, that authority comes from functional registration, operating agreements, and the Reliability Standards. The ability to operate equipment remotely does not change the source or extent of that authority.

The Reliability Coordinator sits at the top. The NERC Glossary describes it as the entity that is the highest level of authority responsible for the Reliable Operation of the Bulk Electric System, with the Wide Area view and the authority to prevent or mitigate emergency operating situations. A remote or virtual arrangement does not dilute that authority. A Control Center performing Reliability Coordinator functions has to make sure its remote arrangements never become a barrier to issuing directives clearly and getting prompt confirmation from the entities that receive them.

4.2 Transfers of Control

In remote operations, control is sometimes transferred, for example from a primary site to a backup or alternate site. Uncertainty during that transition can cause confusion, slower recovery, or conflicting instructions to equipment, and each of those is a reliability risk.

EOP-008-2 makes the transfer a planned event for Reliability Coordinators, Balancing Authorities, and Transmission Operators. The Operating Plan for backup functionality must include Operating Procedures, including decision authority, for deciding when to implement it (R1.4). It must set a transition period of two hours or less (R1.5). It must describe the actions to be taken during the transition, including a list of all entities to notify when operating locations change and the roles of the personnel involved (R1.6). A copy of the current plan must be available at both the primary control center and the backup location (R2).

4.3 Operating Boundaries

Operating boundaries are the limits within which operators may act. Some are technical, such as System Operating Limits. Some are organizational, such as jurisdictional lines and contracts. In remote systems, where an operator may be controlling equipment hundreds of miles away, both kinds need to be written down and visible at the operating position.

Coordination is part of authority. Each operator has to know its own role and the effect its actions can have on other systems and other registered entities. In remote settings, the conditions for conversation and the use of formal communication protocols are different. COM-002-4 requires Balancing Authorities, Reliability Coordinators, and Transmission Operators to maintain documented communications protocols for issuing and receiving Operating Instructions, and to confirm or reissue oral two-party Operating Instructions during an Emergency, or take an alternative action if a response is not received or the instruction is not understood. A Generator Operator that receives one during an Emergency must repeat it back or ask for it to be reissued.

4.4 Emergencies Test the Structure

Emergencies put the most stress on authority and coordination. During a disturbance, operators act under time pressure with incomplete information. A remote arrangement can blur who is in charge unless the operating procedures and escalation paths were settled beforehand.

The standards do not prescribe how to implement authority and coordination for remote locations. They set requirements for coordination, communication, and compliance with directives in general. How far to centralize or distribute control is the registered entity's decision, as long as authority and coordination hold.

Chapter Summary

Authority and coordination are as important in remote and virtual control centers as in a traditional room. Distance does not change the authority or boundaries of a function; it raises the level of coordination required. A defined authority structure, disciplined communication practices, and planned transfer procedures are what keep remote operations reliable.

From the Field

Control authority does not decentralize because the seat moved. The authority is still concentrated; only the seat is distributed. Coordination across distributed operators requires more discipline, not less. The hallway conversation that resolved a question at the physical control center has to be replicated explicitly at the remote one.

5 Reliability Risks and Failure Modes in Remote Environments

Remote and virtual control environments carry their own reliability risks because they have different dependencies, interfaces, and failure modes. The risk analysis has to be done on their terms, without assuming the answer in either direction.

5.1 Telecommunications Dependency

The largest single risk in remote operations is dependence on telecommunications. Operational control, situational awareness, and coordination among personnel all assume the networks, including voice, will be available. A failure of the underlying communication infrastructure, whether from physical damage, a wiring or configuration error, or an external event, can quickly cut the operator's knowledge of the system and ability to respond, even when nothing in the electrical system has failed.

5.2 Latency and Data Quality

Operating from a distance usually means more network hops, more aggregation points, and more interfaces. Poor quality of service brings delay, packet loss, and uneven update rates, all of which can blur the operator's picture of the real-time system and slow the response to a developing problem.

5.3 Concentration and Single Points of Failure

Remote models that are not designed for redundancy can concentrate control functions, communication links, or data services at one point. Consolidation saves money and can improve efficiency, but unless redundancy and separation are designed in, it also raises the consequence of a single site failure.

EOP-008-2 R6 addresses one version of this directly. Reliability Coordinators, Balancing Authorities, and Transmission Operators must have primary and backup functionality that do not depend on each other for the control center functionality required to maintain compliance. A shared virtualization cluster, a single authentication service, or one telecom carrier serving both primary and backup can quietly defeat that independence.

5.4 Human Factors and Transitions

Physical separation from colleagues, field crews, and equipment can change how well people communicate, how much they share an understanding of the situation, and how workload is redistributed. Operators rely more on formal communication and less on nonverbal cues, which can affect crew coordination during abnormal conditions.

Transitions are their own class of failure. Moving control from a primary to a backup site, or from a central site to remote positions, is not always well defined. When a transfer does not go cleanly, there can be confusion about which site is in control, and that confusion costs time in an emergency.

5.5 Cyber Events Are Reliability Events

Cybersecurity is often managed as a separate risk, but a cyber event that affects a remote operating system, a communications network, or a control system has operational consequences. That is a reliability risk, whether the cause is an attack or a technical failure.

5.6 Risk Present Is Not Risk Realized

Separate the presence of a risk from its realization. Remote operations carry different risks, but that does not automatically mean reliability events are more likely. A well-designed remote arrangement can have more redundancy than a single room and a better ability to keep operating if the main facility is lost.

In my view, the existing NERC framework already covers much of the risk of a geographically dispersed operating workforce, through requirements that address outcomes: situational awareness, coordination, communication reliability, emergency response, and backup capability. The standards do not list remote-workplace failure modes. They rest on accountable functions and risk-based oversight. Identifying the failure modes of your own remote environment is what lets you exercise that accountability, and it calls for a system view that accounts for interdependencies, interfaces, and transitions rather than the location of a building.

Chapter Summary

Remote control environments carry reliability risks tied to communications dependency, data quality, concentration of services, human factors, and control transitions. The risks come from a shift in what the system depends on. The functional requirements for awareness, coordination, communication, and backup capability are how the framework addresses them.

From the Field

Remote control is not unreliable. It is differently reliable. The failure modes differ from a physical control center, and the program has to anticipate the new ones. A single-point-of-failure analysis at a remote control center reveals dependencies that were invisible in a physical one. Network paths, video feeds, and authentication services all become potential single points. The new failure modes do not replace the old ones. They add to them, and the program tracks both.

6 Cybersecurity Context for Remote and Virtual Control Centers

In remote and virtual control centers, cybersecurity and reliability are intertwined. As control functions rely more on digital communications, remote access, and distributed computing, cyber risk to those systems becomes risk to the bulk electric system. The cybersecurity program and the operations program each have to account for the other.

6.1 The Attack Surface Moves with the Operator

A remote or virtual control center expands the attack surface of the control systems it uses. New exposures appear, and vulnerabilities that were once mitigated by physical isolation can come back. Equipment and applications that were never reachable from an untrusted network may now be reachable from a less secure remote location, a virtual environment, or a vendor's network.

6.2 How CIP Reaches Control Centers

Within the NERC framework, cybersecurity is addressed mainly through the CIP standards, which cover system identification and categorization, access control, monitoring, incident response, and recovery. Their application depends on the function and impact of the systems, not on whether the control center is physical, remote, or virtual.

CIP-002-5.1a Attachment 1 names Control Centers and backup Control Centers explicitly:

Impact	BES Cyber Systems used by and located at (high) or associated with (medium and low) these Control Centers and backup Control Centers (CIP-002-5.1a, Attachment 1)
High (criteria 1.1–1.4)	Those performing Reliability Coordinator obligations; Balancing Authority obligations for generation of 3,000 MW or more in a single Interconnection or for assets meeting criterion 2.3, 2.6, or 2.9; Transmission Operator obligations for assets meeting criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10; and Generator Operator obligations for assets meeting criterion 2.1, 2.3, 2.6, or 2.9
Medium (criteria 2.11–2.13)	Those not already included in the high impact rating that perform Generator Operator obligations for an aggregate highest rated net Real Power capability of 1,500 MW or more over the preceding 12 calendar months in a single Interconnection; Transmission Operator obligations; or Balancing Authority obligations for generation of 1,500 MW or more in a single Interconnection
Low (criterion 3.1)	Control Centers and backup Control Centers, for BES Cyber Systems not included in the high or medium ratings

For a multi-site renewable or storage Generator Operator, this table settles the first question. An operations center that controls generation at two or more locations is a Control Center. Whether

its BES Cyber Systems are high, medium, or low depends on the criteria above, not on whether the operators are in the building.

The CIP standards do not prohibit any technology. They assume the entity's picture of its systems accounts for the risks its chosen architecture creates. The entity performing the reliability function remains accountable.

6.3 Compliance Is Not Resilience

A cyber incident at a control center can affect reliability directly. Loss of visibility, denial of control commands, or degraded communications can keep operators from managing the system in real time. The cause may be cyber, but the reliability question is the operating impact.

People often blur cybersecurity compliance and cyber resilience. Compliance means the technical and organizational measures meet specific standards. Resilience means the ability to keep or restore functions when something fails. The distinction matters more in remote and virtual control centers, because those arrangements depend more on systems outside the entity's direct physical control. Guidance does not create requirements. The registered entity remains responsible for both the reliability of its assets and the security of its systems, wherever the control functions sit.

Chapter Summary

Remote and virtual control centers depend more on digital communications and remote access, which raises their cyber exposure. The CIP standards address that exposure on a functional basis, and CIP-002 names Control Centers and backup Control Centers at every impact level. A cyber incident at a remote control center is an operating problem, which is why the cyber and operations programs have to be built together.

From the Field

Every remote control center is a CIP scope question. The standards apply wherever the function is performed, and remote means wherever. The home office that doubles as a backup operating position, and the travel laptop used during emergencies, both sit on an access path the program must account for. The standards do not care about convenience; they care about function. The network architecture is the new control center perimeter. Where the wall used to be, the firewall now is. The functional equivalence is real; the engineering required to achieve it is not trivial. A flat network that worked for the physical control center can leave the remote model one compromised endpoint away from full system access. Defense in depth at the network layer is what makes remote control defensible. A single layer of network protection tends to show up in findings, not in resilience.

7 Remote Access, Virtualization, and Cyber Risk Considerations

Remote access and virtualization are now standard parts of control center technology, and they support flexible, resilient, and efficient operations. The cyber risk they carry sits inside existing reliability responsibilities and existing oversight.

7.1 Interactive Remote Access Under CIP-005-7

The NERC 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, originating from a Cyber Asset that is not an Intermediate System and not inside any of the entity's Electronic Security Perimeters or at a defined Electronic Access Point. It can originate from devices owned by the entity, by employees, or by vendors, contractors, or consultants. It does not include system-to-system process communications.

In remote and virtual control centers, that kind of access is often the normal way of operating, not the contingency. CIP-005-7 R2 sets the controls for high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity, and their associated Protected Cyber Assets:

CIP-005-7 R2 Part	Requirement
2.1	For all Interactive Remote Access, use an Intermediate System so the initiating Cyber Asset does not directly access an applicable Cyber Asset
2.2	For all Interactive Remote Access sessions, use encryption that terminates at an Intermediate System
2.3	Require multi-factor authentication for all Interactive Remote Access sessions
2.4	Have one or more methods to determine active vendor remote access sessions, including Interactive Remote Access and system-to-system remote access
2.5	Have one or more methods to disable active vendor remote access

CIP-005-7 R3 adds vendor remote access controls for the Electronic Access Control or Monitoring Systems and Physical Access Control Systems associated with high impact systems and medium impact systems with External Routable Connectivity. For low impact, CIP-003-9, effective April 1, 2026, added Attachment 1 Section 6, which requires methods to determine, disable, and detect malicious communications for vendor electronic remote access.

7.2 Monitoring Who Is Actually Using the Access

Requiring multi-factor authentication is only half the job. CIP-007-6 R4 requires logging, for identification and after-the-fact investigation of Cyber Security Incidents, that includes at minimum detected successful login attempts, detected failed access and login attempts, and detected malicious code (Part 4.1). It requires alerts for security events the entity determines need them, including at minimum detected malicious code and detected failure of Part 4.1 logging (Part 4.2), and retention of those logs for at least the last 90 consecutive calendar days where technically feasible (Part 4.3).

Personnel controls matter as much. CIP-004-7 R5.1 requires a process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and to complete those removals within 24 hours, for high impact systems and medium impact systems with External Routable Connectivity and their associated access control systems. For a dispersed operating staff, that clock runs regardless of where the departing employee happens to be working that day.

7.3 Virtualization

Control centers increasingly host, manage, and monitor systems on shared or virtualized infrastructure. Functions that once ran on dedicated hardware now share hosts, storage, and networks. Virtualization adds flexibility and redundancy, but it can also hide system boundaries and dependencies, which makes them harder to manage from both a security and an operations standpoint.

The CIP standards are catching up. FERC approved the NERC Project 2016-02 virtualization revisions in Docket No. RM24-8-000. Revised versions across the CIP family, including CIP-003-10, CIP-005-8, CIP-007-7.1, and CIP-010-5, and revised Glossary definitions including BES Cyber Asset, Cyber Assets, and Electronic Security Perimeter, take effect July 1, 2028. Until then, the currently enforceable versions apply to virtualized control center systems as they are written.

7.4 Third Parties and Shared Platforms

From a reliability standpoint, remote access and virtualization are not the problem. The problem is what happens to control availability and operator effectiveness when something goes wrong and immediate action is needed. An unexpected loss of access, degraded system performance, or an unexpected interaction between virtualized components can erode situational awareness and slow the response.

The risks that recur are familiar: authentication failures, misconfigurations, software vulnerabilities, and shared infrastructure. A single cyber or technical incident on a common platform or access point can affect several operating processes at once if they all depend on it. Accountability stays with the registered entity performing the reliability function. Using third-party services, shared platforms, or virtual environments does not change that. The entity has to understand what its architecture choices mean for cyber and operating risk.

7.5 Recovery and Restoration

Recovery in virtualized environments deserves attention. Virtualization can make restoration fast, but it can also complicate fault identification and recovery priorities. CIP-009-6 requires recovery plans for high and medium impact BES Cyber Systems, and requires the plans for high impact systems and medium impact systems at Control Centers to be tested at least once every 15 calendar months (R2 Part 2.1). A recovery plan for a virtual control center has to restore the operating function, not just the virtual machines.

Chapter Summary

Remote access and virtualization bring real operating advantages and real cyber and operating dependencies. CIP-005-7, CIP-007-6, CIP-004-7, and CIP-009-6 already govern those dependencies, and the virtualization revisions arrive July 1, 2028. Focus on the effect on the operating function, the remote access controls, and the restoration process rather than on the technology itself.

From the Field

The remote operator has the same access to the system as the operator in the primary room. Remoteness does not reduce the privilege; it complicates verifying who is actually using it. Multi-factor authentication is necessary but not sufficient. The audit looks at how authentication is monitored, not just whether it is required. Personnel access controls in a remote model have to anticipate scenarios the physical model never did: shared devices, family members in the room, intermittent connectivity. The program has to have a written position on each.

8 Oversight, Registration, and Applicability Considerations

Oversight, registration, and applicability for remote and virtual control centers rest on the functions performed and their impact on the Bulk Electric System. Keeping that in view prevents most of the confusion entities run into when they move control work out of a traditional room.

8.1 Registration Follows Function

Functional registration remains the basis of reliability responsibility. Entities are registered for the functions they perform, such as Transmission Operator, Balancing Authority, Reliability Coordinator, or Generator Operator. Where the personnel or systems sit does not change the registration. An entity can operate remotely without changing its registered functions, and moving operators does not by itself put the entity into a new function.

8.2 Applicability and How Compliance Is Shown

Each Reliability Standard defines the functions and Facilities to which it applies. Some apply to specific systems, such as BES Cyber Systems at Control Centers. Others apply to activities that are part of control center operations, such as issuing instructions, communicating, maintaining situational awareness, and coordinating, wherever they are performed.

The standards do not distinguish between a traditional control room and a remote or virtual one. Changing the configuration can, however, change how the entity demonstrates compliance. When work moves to remote locations, the evidence that Operating Instructions were communicated and confirmed, or that the operator could respond, may look different. That is a question of implementation and documentation. The underlying requirement does not change.

8.3 Delegation Does Not Transfer Responsibility

Shared resources, remote control, and third-party services can make roles hard to untangle. A contractor may do most of the work. The registered entity is still the one on the NERC Compliance Registry, and it is still responsible for compliance. Delegating a task does not delegate the obligation.

Most remote operating models include a backup or alternate control center. When control authority moves to that location, oversight of it does not change. The entity must always be able to deliver the required communication, coordination, and command and control from whichever location holds control of the system.

Remote operations also raise registration and applicability questions when assets span wide areas or several Regional Entity footprints. Those are handled within the existing registration process and the NERC Rules of Procedure. There is no separate regime for remote operations.

8.4 What Changes in 2028

The next applicability change for Control Centers is already approved. CIP-002-8 takes effect July 1, 2028, and supersedes CIP-002-7, which is retired immediately before CIP-002-8 takes effect. With it comes the revised Control Center definition described in Section 2.1, and a revised criterion 2.12 that uses a weighted value of transmission lines monitored and controlled, with a threshold of 6,000. A Transmission Owner that operates switching remotely without being registered as a Transmission Operator should be working that analysis now.

Chapter Summary

Registration and applicability for remote control centers depend on the functions performed, not on geography or technology. Remote operation does not change an entity's registration or create new obligations, though it can change how compliance is demonstrated. The revised Control Center definition and CIP-002-8 on July 1, 2028 are the next change to plan for.

9 Compliance Monitoring and Enforcement in Remote Operations

Monitoring and enforcement of the Reliability Standards work the same way for remote and virtual control centers as for traditional ones. The question is whether the requirements are met, not how the control environment is built.

9.1 The Same Monitoring Tools

The NERC Compliance Monitoring and Enforcement Program, Appendix 4C to the NERC Rules of Procedure, uses the same processes for every registered entity: Compliance Audits, Self-Certifications, Spot Checks, Compliance Investigations, Self-Reports and Self-Logging, Periodic Data Submittals, and Complaints. Any of them can reach remote control arrangements when those arrangements bear on a requirement. Running a remote operation is not, by itself, a trigger for enforcement.

Each year NERC and the Regional Entities publish an ERO CMEP Implementation Plan that identifies the risk elements, and the related standards and requirements, that Compliance Enforcement Authorities should prioritize. Oversight goes where the risk is, and not every remote arrangement carries the same risk.

9.2 What the Evidence Looks Like

Evidence for remote operations differs only in form. Expect an audit team to look at communication procedures, operating authority, and backup and transfer-of-control documentation, along with the CIP architecture behind the access. For a Reliability Coordinator, Balancing Authority, or Transmission Operator, that typically means:

- The EOP-008-2 Operating Plan for backup functionality, the copies at both the primary and backup locations (R2), the annual review and approval (R5), and the annual test record showing the transition time and at least two continuous hours on backup functionality (R7).
- COM-001-3 records showing each monthly test of Alternative Interpersonal Communication and the response to any failed test (R9).
- Network diagrams and architecture documents showing the Intermediate System, where encryption initiates and terminates, and the authentication factors used for Interactive Remote Access (CIP-005-7 R2).
- Event logs and alerting configuration for those access paths (CIP-007-6 R4) and access removal records (CIP-004-7 R5).

When a disturbance occurs, an event review may ask whether the remote arrangement affected the operator's awareness or the speed and quality of the response. Any finding of noncompliance rests on the requirement and the evidence, not on the fact that the work was

done remotely. Mitigation expectations focus on fixing the identified problem and reducing the risk.

9.3 What the 2025 Data Shows

NERC's ORCP and CMEP Annual Report, published February 11, 2026, reports that the most frequently reported CIP noncompliance in 2025 involved CIP-010, CIP-007, and CIP-004, all high-volume, high-frequency conduct. NERC's enforcement cause codes point to lacking or deficient policies and procedures as the leading root cause for all three.

Those three standards are exactly where remote operations add load: configuration baselines for more endpoints and virtual hosts, security event logging across more access paths, and access authorization and removal for a dispersed workforce. In my view, a remote operations program that has not rewritten its procedures for those three standards is carrying the risk NERC is describing.

9.4 Risk-Based Oversight

Risk-based oversight is how the ERO approaches remote operations, as it is how it approaches everything else. Oversight is proportionate and informed, not prescriptive. Applying the same compliance monitoring and enforcement to every operating model supports operating flexibility while keeping accountability where it belongs, with the registered entity.

Chapter Summary

Compliance monitoring and enforcement for remote control centers rest on the functions the facility performs, not its physical form. Audit teams look at the arrangements for situational awareness, communication, authority, and response, using the standard CMEP processes. The 2025 enforcement data points straight at the procedures remote operations stress the most.

From the Field

The Region audits remote operations the same way it audits physical operations. The evidence is different; the standards are the same. Documentation that the remote operator's environment meets CIP expectations has to exist before the audit asks. Building it during the audit is too late. If I were pre-auditing a remote control center, I would start with three things: the asset and access-path inventory, Interactive Remote Access logging, and the physical security position for remote workstations.

10 Disturbance Experience and Reliability Lessons

Operating experience is the best teacher on remote and virtual control centers. NERC's EMS event analysis is the closest thing the industry has to hard data on this question, and it found one direct link to remote work.

10.1 What the EMS Data Shows

In December 2021, NERC published Analysis and Risk Mitigations for Loss of EMS Functions (2018–2020), building on an earlier NERC EMS Working Group reference document on the risks and mitigations of losing EMS functions. NERC found that energy management systems were highly reliable over the period and that loss of EMS functions did not lead to loss of generation, transmission lines, or customer load. Reported EMS events fell from 88 in 2018 to 74 in 2019 and 58 in 2020, and the median outage duration stayed near one hour.

Loss of SCADA became the most prevalent EMS failure in 2020, at about 52 percent of the 58 events reported that year. Across all 203 processed events, NERC identified Management/Organization as the leading root cause in 67 of them, pointing to job scoping, peer review, and change management rather than the technology itself.

10.2 Remote Work in 2020

The same report ties some of the 2020 problems directly to remote operation. NERC found delays in response times due to inadequate plans for an abnormal working environment that included working remotely and having to implement split shifts at backup control centers.

NERC's considerations for entities followed from that. It called it essential to develop and practice plans and procedures for an abnormal working environment, such as working remotely, and to improve the materials and tools that let shifts monitor and control the system from backup control centers. It also called for regular testing of backup generators, uninterruptible power supplies, and associated switching, and for planned maintenance of network devices in line with current vendor and security bulletins.

10.3 Remote Capability as a Strength

The upside is the reason EOP-008-2 exists: backup functionality lets an entity keep operating when severe weather, fire, flooding, or physical damage takes a primary facility out of service. It is also why a well-built remote capability can raise availability rather than lower it.

10.4 Transitions and Human Factors

Transitions between operating locations come up repeatedly. Changing who holds control, especially under time pressure, touches roles and responsibilities, the alignment of control

systems at both sites, and crew readiness. Human factors come with it. Distance cuts the informal interaction between personnel, which in turn affects how often, and how well, formal communication is used to deal with emerging events.

My read of the record is that remote and virtual control centers can increase reliability or expose new weaknesses, depending on how interdependencies, transitions, and human factors are handled. The architecture alone does not decide it.

Chapter Summary

NERC's EMS event analysis found EMS performance strong overall, with loss of SCADA the leading failure in 2020 and management and organizational causes leading overall. It also found response delays tied to inadequate plans for remote work and backup-site shifts. Remote capability helps when the primary site is lost; unpracticed transitions hurt.

From the Field

A backup control center used to be a building. Now it is an operating model. The reliability question is whether the operating model has been exercised, not whether the second building exists. EOP-008-2 sets an annual test as the minimum. In my view, a remote control center should fail over more often than that, because the system is more dynamic and the test cadence has to match.

11 Common Misconceptions About Remote Control Centers

Misconceptions about remote and virtual control centers tend to obscure, rather than clarify, what the standards and enforcement practice actually require. Six come up often.

11.1 "Remote Control Centers Reduce Reliability"

Reliability depends on how the elements of the system perform, not on where they are. A remote location does not, by itself, affect reliability, provided control, awareness of operating conditions, communication, and coordination are maintained.

11.2 "Remote Operation Needs Its Own Standards"

Remoteness is not a reason to impose new reliability obligations or to argue that the existing standards must change. The standards that apply depend on the functions performed and their impact on the Bulk Electric System, not on where the operating personnel sit. Remote and virtual operation are different ways of doing control center work, not grounds for different standards. Where the risk did change, the framework adjusted requirements it already had, as CIP-012-2 did for data moving between Control Centers and as the virtualization revisions will do in 2028.

11.3 "Cybersecurity Is Separate from Reliability"

The two are closely linked. A cyber incident that disrupts remote operations, communications, or control systems has operating consequences, and the existing standards and oversight processes are built to handle that link.

11.4 "Remote Access Is Inherently Insecure"

Remote access adds potential failure points. It also preserves control if the primary access points, such as the panels in a protected facility, are compromised or lost. The risk rises when remote access is implemented in a way that raises it: without an Intermediate System, without multi-factor authentication, without logging, or without vendor session controls.

11.5 "Regulators Prefer a Particular Design"

No Reliability Standard prescribes a control center architecture, and neither NERC nor FERC requires one. The question is whether the entity has the controls in place to meet the reliability and CIP requirements that apply to it.

11.6 "Consolidation Means Loss of Control"

Consolidation and virtualization carry concentration risk if they are managed poorly, and they can also improve coordination and use of resources. Either way, reliability rests on the same fundamentals: redundancy, diversity, and sound operating procedures.

Chapter Summary

Remote control centers do not inherently reduce reliability, do not need their own standards, and are not disfavored by regulators. Reliability expectations stay function-based and technology neutral. What gets assessed is situational awareness, authority, coordination, and timely response, wherever the work is done.

From the Field

"We are a remote operation, so the standards do not fully apply" is the misunderstanding that produces findings. "The third party hosts the operation, so they are accountable" is the next one. The registered entity is accountable; outsourcing the operation does not outsource the obligation. Then there is "We covered this in our IT security program." IT security and CIP overlap, but they are not equivalent. CIP has specific evidence requirements that general IT security does not.

12 Remote Operations in Practice and Ongoing Evolution

Remote and virtual control centers are no longer experiments. They are part of normal bulk power system operations, driven by technology, workforce change, emergency preparedness, and cost.

12.1 Remote as Normal Operations

Running remote capability only as a contingency is a mistake. Routine use builds more predictable responses to emergencies, steadier authority and coordination relationships, and a better understanding of what the monitoring and control systems can and cannot do. A capability exercised every week is far more trustworthy on a bad day than one opened once a year for the EOP-008-2 test.

12.2 What Is Already Scheduled

The requirements keep moving, and the dates are known:

Date	Change
April 1, 2026	CIP-003-9 in effect, adding low impact vendor electronic remote access controls (Attachment 1, Section 6)
July 1, 2026	CIP-012-2 in effect for Real-time Assessment and Real-time monitoring data transmitted between Control Centers
July 1, 2028	Virtualization revisions across the CIP family, including CIP-003-10, CIP-005-8, CIP-007-7.1, and CIP-010-5; CIP-002-8, which supersedes CIP-002-7; and the revised Control Center definition
October 1, 2028	CIP-015-1 internal network security monitoring for high impact systems and medium impact systems with External Routable Connectivity
July 1, 2029	CIP-003-11 low impact authentication, protection of authentication information in transit, and malicious communication detection

Design decisions made now, such as a new virtualization platform, a new remote access gateway, or a new backup site, will still be in service when the 2028 and 2029 changes take effect. Build to them.

12.3 The People Side

Reliability in remote operations also depends on how the organization works: training, communication habits, and clarity about roles. PER-005-2 requires a systematic approach to

training for System Operators, and COM-002-4 requires annual assessment of adherence to communications protocols for Balancing Authorities, Reliability Coordinators, and Transmission Operators. Beyond those, much of what makes remote work succeed, such as shift handoff discipline and how a dispersed crew builds a shared picture, sits outside the standards and inside the operating culture.

12.4 The Principle Holds

The spread of remote and virtual control centers keeps proving the founding idea of the NERC framework: standards built on functional accountability can absorb new ways of working. Because the standards focus on performing functions rather than on locations or methods, practice can evolve without rewriting the rules. Remote control done well adds redundancy to system operations. Done well means the dependencies, authority, and coordination have been thought through, and the remote access follows the security requirements as written.

Chapter Summary

Remote and virtual control centers are now an ordinary part of BES operations. Their reliability depends on treating them as normal operations, managing their dependencies, and running the work with discipline. Oversight remains risk-based, and the scheduled CIP changes through 2029 are the planning horizon for any remote operations design.

Glossary

Definitions marked as NERC Glossary terms are quoted or closely paraphrased from the Glossary of Terms Used in NERC Reliability Standards as currently enforceable. Other entries describe how this reference uses a term and do not modify any NERC definition.

Term	Meaning in this paper
Alternative Interpersonal Communication	Any Interpersonal Communication that is able to serve as a substitute for, and does not utilize the same infrastructure (medium) as, Interpersonal Communication used for day-to-day operation. (NERC Glossary)
Balancing Authority	The responsible entity that integrates resource plans ahead of time, maintains Demand and resource balance within a Balancing Authority Area, and supports Interconnection frequency in real time. (NERC Glossary)
Bulk Electric System (BES)	Unless modified by the inclusions and exclusions in the definition, all Transmission Elements operated at 100 kV or higher and Real Power and Reactive Power resources connected at 100 kV or higher; it does not include facilities used in the local distribution of electric energy. (NERC Glossary)
Control Center	One or more facilities hosting operating personnel that monitor and control the BES in real time to perform the reliability tasks, including their associated data centers, of a Reliability Coordinator, a Balancing Authority, a Transmission Operator for transmission Facilities at two or more locations, or a Generator Operator for generation Facilities at two or more locations. The revised definition effective July 1, 2028 adds certain Transmission Owner facilities with SCADA control at two or more locations. (NERC Glossary)
Critical Infrastructure Protection (CIP) standards	The NERC Reliability Standards, CIP-002 through CIP-015, that address the cyber and physical security of BES Cyber Systems and related assets.
External Routable Connectivity	The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection. (NERC Glossary)
Interactive Remote Access	User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol, originating from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeters or at a defined Electronic Access Point. It does not include system-to-system process communications. (NERC Glossary)
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. (NERC Glossary)

Term	Meaning in this paper
Reliability Coordinator	The entity that is the highest level of authority who is responsible for the Reliable Operation of the Bulk Electric System, has the Wide Area view, and has the operating tools, processes, and procedures, including the authority to prevent or mitigate emergency operating situations. (NERC Glossary)
Remote operations	As used here, operations in which some or all control center activities are performed away from the facility that normally hosts them or from the equipment being controlled.
Risk-based oversight	As used here, the ERO approach of focusing monitoring and enforcement on the entities, standards, and requirements that pose the greatest risk to reliability, as reflected in the annual ERO CMEP Implementation Plan.
Situational awareness	As used here, the ability of operating personnel to perceive, interpret, and anticipate the state of the system well enough to make timely and effective operating decisions.
Transmission Operator	The entity responsible for the reliability of its local transmission system, and that operates or directs the operations of the transmission Facilities. (NERC Glossary)
Virtual control environment	As used here, a control center configuration in which operating systems run on virtualized or distributed infrastructure rather than dedicated physical hardware.

How Energy Compliance Can Help

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

- CIP applicability and scope analysis (CIP-002 through CIP-014)
- Cyber asset and BES Cyber System identification and impact classification
- Electronic Security Perimeter and Physical Security Perimeter boundary analysis
- CIP governance and program assessments
- Integration of cybersecurity oversight with broader reliability programs
- Audit and enforcement support for CIP findings (non-advocacy)
- CIP framework reviews, gap analyses, and improvement plans
- Training focused on CIP framework, requirements, and audit expectations
- Executive and board-level CIP awareness briefings

Around that core, EC provides NERC compliance program support, interpretation, and audit preparation; audit defense with Notice of Penalty response and settlement posture; senior advisory on complex reliability questions, including EOP-008 backup functionality and COM-001 communications design for remote operations; 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 fits the non-CIP evidence a remote program generates, such as EOP-008-2 backup functionality test records and COM-001-3 monthly test records. 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 a solar, wind, or storage fleet run from a remote operations center, the operations data path is part of the Control Center analysis in Chapter 6.

Start with one question: could you show an auditor, today, every path by which an operator reaches your control systems from outside the room? If the answer is no, 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.

Learn more at energycomplianceinc.com.

Sources and Authorities

- North American Electric Reliability Corporation (NERC), Glossary of Terms Used in NERC Reliability Standards (Control Center, Interactive Remote Access, Intermediate System, External Routable Connectivity, Alternative Interpersonal Communication, Real-time Assessment, and the functional entity definitions). https://www.nerc.com/glossary-of-terms
- 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, Attachment 1 (effective April 1, 2026). https://www.nerc.com/globalassets/standards/reliability-standards/cip/cip-003-9.pdf
- NERC, Reliability Standard CIP-004-7, Cyber Security: Personnel & Training, Requirement R5. 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), Requirements R2 and R3. https://www.nerc.com/globalassets/standards/reliability-standards/cip/cip-005-7.pdf
- NERC, Reliability Standard CIP-007-6, Cyber Security: System Security Management, Requirement R4. https://www.nerc.com/globalassets/standards/reliability-standards/cip/cip-007-6.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-012-2, Cyber Security: Communications between Control Centers (effective July 1, 2026). https://www.nerc.com/globalassets/standards/reliability-standards/cip/cip-012-2.pdf
- NERC, Reliability Standards, CIP family listing (effective and future enforcement dates, including CIP-015-1). https://www.nerc.com/standards/reliability-standards/cip
- NERC, Project 2016-02 Modifications to CIP Standards, Implementation Plan (virtualization revisions; FERC Docket No. RM24-8-000). https://www.nerc.com/standards/reliability-standards-under-development/2016-02-modifications-to-cip-standards
- Federal Energy Regulatory Commission (FERC), North American Electric Reliability Corporation; Order Approving Reliability Standard CIP-002-8, Docket No. RD25-8-000 (issued March 19, 2026; 91 FR 14013, March 24, 2026). https://www.govinfo.gov/content/pkg/FR-2026-03-24/pdf/2026-05715.pdf

- FERC, Order No. 918, Critical Infrastructure Protection Reliability Standard CIP-003-11, Cyber Security: Security Management Controls, Docket No. RM25-8-000 (March 19, 2026). https://www.govinfo.gov/content/pkg/FR-2026-03-24/pdf/2026-05711.pdf
- NERC, Reliability Standard EOP-008-2, Loss of Control Center Functionality (effective April 1, 2019). https://www.nerc.com/globalassets/standards/reliability-standards/eop/eop-008-2.pdf
- NERC, Reliability Standard EOP-004-4, Event Reporting, Attachment 1. https://www.nerc.com/globalassets/standards/reliability-standards/eop/eop-004-4.pdf
- NERC, Reliability Standard COM-001-3, Communications (effective October 1, 2017). https://www.nerc.com/globalassets/standards/reliability-standards/com/com-001-3.pdf
- NERC, Reliability Standard COM-002-4, Operating Personnel Communications Protocols (effective July 1, 2016). https://www.nerc.com/globalassets/standards/reliability-standards/com/com-002-4.pdf
- NERC, Reliability Standard PER-005-2, Operations Personnel Training. https://www.nerc.com/globalassets/standards/reliability-standards/per/per-005-2.pdf
- NERC, Rules of Procedure, Appendix 4C, Compliance Monitoring and Enforcement Program (effective May 19, 2022), Sections 3.0 and 4.0. https://www.nerc.com/globalassets/who-we-are/rules-of-procedure/appendix-4c.pdf
- NERC, ORCP and CMEP Annual Report (February 11, 2026). https://www.nerc.com/globalassets/programs/enforcement/cmep-and-vegetation-reports/2025-orcp-and-cmep-annual-report.pdf
- NERC, Analysis and Risk Mitigations for Loss of EMS Functions (2018–2020) (December 2021). https://nerc.com/pa/rrm/ea/PapersDocumentsAssessmentsDL/Analysis_and_Risk_Mitigations_2018-2020.pdf
- FERC, News Release, FERC, NERC Provide Industry Guidance to Ensure Grid Reliability Amid Potential Coronavirus Impacts (March 18, 2020). https://www.ferc.gov/news-events/news/ferc-nerc-provide-industry-guidance-ensure-grid-reliability-amid-potential

© Energy Compliance, Inc. · EC-WP-206 · October 2026