CYBERSECURITY · CIP SERIES · EC-WP-207

CIP Evidence: Building Audit-Defensible Programs

Evidence is the difference between a defensible CIP program and a binder full of screenshots.

A CIP control that left no evidence is, to an audit team, a control that never ran. This reference explains what CIP evidence is, how audit teams request and sample it, and why it ages, drifts and fails to reconcile across standards. It closes with five design principles for an evidence program that holds up for the full audit period.

energycomplianceinc.com

OCTOBER 2026

Disclaimer & Legal Notice

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

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

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

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

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

Foreword

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

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

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

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

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

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

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

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

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

Rob Smith

Founder and Principal, Energy Compliance, Inc.

Executive Summary

CIP compliance is a documentation discipline. The control might be perfect; if the evidence isn't there, the auditor produces a finding. Across the CIP standards in force today, CIP-002 through CIP-014, the audit outcome turns on whether evidence was captured, organized, and retained, and whether it actually demonstrates what the program claims it demonstrates. Appendix 4C of the NERC Rules of Procedure puts it plainly: the entity's data and information must show compliance for the entire period the audit covers. Programs that build evidence as a live deliverable tend to pass cleanly. Programs that assemble it after the fact tend to get caught by what they didn't preserve.

- **Evidence is the backbone of CIP compliance.** Without it, every control is a claim. With it, every claim is defensible.
- **The data points at process, not technology.** NERC's 2025 annual report lists CIP-010, CIP-007, and CIP-004 as the most frequently reported CIP noncompliance, and names lack of or deficient policies and procedures as the leading root cause for CIP issues. In my view, many of those findings are evidence gaps that look like control failures from the auditor's seat.
- **Evidence ages.** A procedure that produced good evidence two years ago may produce nothing defensible today if the system, the standard version, or the people behind it changed.
- **Sampling is how the auditor reads the program.** Under the ERO Enterprise CIP Evidence Request Tool, the populations an entity reports at Level 1 become the pool the audit team samples for Level 2 implementation evidence.
- **Cross-standard reconciliation is where programs leak findings.** CIP-007 patch records have to match CIP-010 baselines, and both have to match the CIP-002 categorization.
- **Documentation that exists only in someone's head isn't documentation.** It's a single point of evidence failure.
- **Two levels of ambition.** An evidence program designed to answer the next request for information is good. One designed to demonstrate ongoing operation across the whole audit period is audit-grade.

1 What CIP Evidence Actually Is

CIP evidence is anything that would convince an objective reviewer that the control existed, executed correctly, and was applied consistently.

1.1 A Body of Records, Not a Single Artifact

CIP evidence is the body of records, logs, screenshots, configurations, signatures, attestations, and metadata that, taken together, demonstrate that a CIP requirement was met. Knowing what counts for each requirement is foundational, and a program that runs the same evidence template across every standard has misframed the work.

1.2 What the Standards Say Counts

Each CIP standard carries a Measures column next to its requirements. CIP-007-6 explains what that column is for: the measures "provide examples of evidence," serve as guidance on acceptable records, "and should not be viewed as an all-inclusive list."

For the Electronic Security Perimeter, CIP-005-7 suggests a list of every ESP with the applicable Cyber Assets inside it (Part 1.1), network diagrams showing all external routable communication paths and the identified Electronic Access Points (Part 1.2), and a rule list showing that only permitted access is allowed and that each rule has a documented reason (Part 1.3). For patching, CIP-007-6 requires a patch evaluation at least once every 35 calendar days (Part 2.2) and, within 35 calendar days of completing each evaluation, either the patch applied or a dated mitigation plan created or revised (Part 2.3). The evidence is the source list, the dated evaluations, the installation records, and the dated plans.

1.3 Four Tests Every Artifact Must Pass

In my view, the auditor's test for evidence is consistent across the CIP standards. Evidence has to be **authentic**: provably from the system or process it claims to document. It has to be **contemporaneous**: created when the control executed, not assembled afterward. It has to be **complete**: covering the full audit period and the full scope of the requirement. And it has to be **coherent**: internally consistent and reconciled across related artifacts.

Programs that internalize those four tests build evidence as a continuous output of operations. One failure deserves early attention: evidence that existed but wasn't preserved when the system that generated it was decommissioned, replaced, or reconfigured. The ERT's Cyber Asset tab asks for each applicable Cyber Asset the entity had compliance responsibility for within the audit period, so a device retired last year can still be in the population.

> **From the Field**
>
> Evidence assembled after the fact rarely passes the contemporaneity test, and the auditor can tell.

2 The Evidence Inventory Most Programs Don't Have

Programs that don't catalog their evidence can't see what's missing until the auditor asks.

2.1 Evidence Versus an Inventory of Evidence

Most CIP programs have evidence. Few have an evidence inventory. The difference shows up at audit. An inventory tells the program what evidence exists, where it's stored, who maintains it, how long it's retained, and which CIP requirements it supports. Without one, evidence is a series of artifacts the program hopes will be enough when the audit asks.

2.2 Building and Maintaining It

Building an evidence inventory is a one-time effort followed by ongoing maintenance. The one-time effort: catalog every evidence source that supports any CIP requirement, document its retention, identify the requirement or requirements it satisfies, and assign an owner. The ongoing maintenance: every operational change that affects an evidence source triggers an inventory update.

Retention deserves its own column. The CIP standards set a floor. CIP-007-6, CIP-010-4, and their companions require evidence of each requirement to be kept for three calendar years, and longer for information related to a noncompliance until mitigation is complete and approved. The same sections warn that where the retention period is shorter than the time since the last audit, the Compliance Enforcement Authority may ask for other evidence covering the full period. Appendix 4C, Section 4.1.3.2, starts the audit period the day after the End Date of the prior Compliance Audit. In my view, the inventory should key retention to the audit period, not just to the three-year minimum.

2.3 What It Pays and What It Costs to Skip

The payoff at audit is real. The program can answer evidence requests in hours instead of days because the location of each record is known. It can demonstrate completeness by pointing to the inventory instead of searching for gaps in real time. And it finds its gaps early, during the inventory exercise, when correction is cheap.

The cost of skipping it is just as real. Response times stretch. Gaps surface during the audit, when it is too late to fix them for the audit period. The program looks less mature to the audit team.

> **From the Field**
>
> An evidence inventory turns evidence from artifacts into infrastructure.

3 Evidence Architecture: Built or Built Up

Evidence systems are either designed for compliance or accreted from operational artifacts. The two have different audit profiles.

3.1 Designed Evidence Systems

Evidence comes from somewhere. In some programs it comes from systems built to produce compliance evidence: automated logging, continuous monitoring, structured documentation workflows. In others it comes from operational systems that happen to produce records that can serve as evidence. The difference shapes the audit experience.

Designed evidence systems produce consistent, complete, contemporaneous records. The evidence comes out the way it was designed to, and the audit reads it cleanly. These systems take investment up front and ongoing maintenance. In my view, they pay it back in audit efficiency and in findings avoided.

3.2 Accreted Evidence Systems

Accreted evidence systems use what's available. Operational logs that happen to capture compliance-relevant events. Email trails that happen to document approvals. Calendar entries that happen to show meeting frequency. The evidence is real, but it's irregular, sometimes incomplete, and often needs interpretation. The audit reads it with more friction.

3.3 When the Difference Surfaces

Programs that have grown into accreted evidence systems often don't notice until the audit. The evidence has been "adequate" for years, in the sense that no auditor has flagged it. Then a more thorough audit cycle arrives and the gaps become visible. Fixing them means more than repairing individual evidence sources. It means redesigning the evidence architecture, which takes longer and costs more than designing it properly would have.

> **From the Field**
>
> Designed evidence systems require investment. Accreted evidence systems require explanation. Redesigning one after a finding usually costs more than building it right the first time.

4 Sampling: What the Auditor Actually Asks For

CIP audits sample, and the samples are drawn from what the entity itself reports.

4.1 How the Evidence Request Tool Works

The audit team doesn't review every artifact in the audit period. It samples. For CIP audits, the ERO Enterprise publishes a common request for information that every Region can use, the CIP Evidence Request Tool (ERT). Its Level 1 tab asks for two kinds of evidence: completed detail tabs for the CIP standards in scope, which "form populations for sample selection," and general requests for the programs, processes, and procedures behind those standards. Level 2 then asks for detailed implementation evidence for the specific items the audit team sampled.

The detail tabs cover BES Assets, Cyber Assets, Electronic Security Perimeters, Electronic Access Points, Physical Security Perimeters, Transient Cyber Assets, Removable Media, BES Cyber System Information, personnel, reuse and disposal, Cyber Security Incidents, procurement, and, optionally, low impact Cyber Assets. Every row an entity enters is a candidate for a Level 2 request. The ERT also notes that requests may include requirements subject to future enforcement.

4.2 What a Good Sample Probes

A sample is a set of questions about the program, and a well-built sample asks several at once. Coverage across asset classes. Concentration on the highest-risk systems. Spread across the audit period to catch drift. The edges of scope and categorization. Entries that look unusual. Each probes a different part of program quality.

Programs that anticipate sampling prepare differently. They make sure every asset category, every time period, every categorization boundary, and every exception has clean, defensible evidence.

4.3 The First Sample Sets the Tone

The audit team's view of the program is shaped by the samples it draws. In my view, a first sample that comes back clean frames the program favorably, and one that comes back with problems invites a closer look and more requests. Programs that handle the first sample well tend to have shorter audits. Programs that don't often have audits that grow.

> **From the Field**
>
> Your Level 1 population is the audit team's sample pool. Sample it yourself first.

5 Evidence Aging and the Refresh Discipline

Evidence has a useful life.

5.1 Why Evidence Ages

CIP standards revise. Equipment gets replaced. Systems get reconfigured. People rotate. Each event ages the evidence base.

The CIP family is in the middle of exactly that kind of change. CIP-003-9 became enforceable on April 1, 2026, and CIP-012-2 on July 1, 2026. NERC lists the virtualization revisions to most of the family, including CIP-003-10, CIP-004-8, CIP-005-8, CIP-007-7.1, and CIP-010-5, as effective July 1, 2028. CIP-002-8 takes effect the same day. FERC approved it in Docket No. RD25-8-000 and approved retiring CIP-002-7 immediately before CIP-002-8 takes effect, so CIP-002-8 is the categorization standard from that date. CIP-015-1, internal network security monitoring, follows on October 1, 2028. Evidence designed against today's text will need a refresh pass before each of those dates.

5.2 Two Kinds of Refresh

The refresh discipline has two parts. The first is periodic re-validation: at defined intervals, evidence is re-examined to confirm it still supports the requirement it was captured for. CIP-002-5.1a already builds this in for categorization, requiring a review of the identifications at least once every 15 calendar months and approval by the CIP Senior Manager or delegate on the same cycle.

The second is change-triggered refresh: any operational change that affects an evidence source triggers a review. Replacing equipment means re-capturing equipment-specific evidence. Reconfiguring a system means re-documenting it. A personnel change means handoff documentation. For baselines, CIP-010-4 Part 1.3 makes this mandatory: a change that deviates from the baseline requires a baseline update within 30 calendar days of completing the change.

5.3 What Stale Evidence Looks Like at Audit

Programs without a refresh discipline accumulate stale evidence, and the accumulation stays invisible until the audit. Then the auditor compares evidence dates against system change records and finds, say, a 2022 evidence package describing a configuration retired in 2023.

In my view, refresh is cheap and stale evidence is not. A quarterly evidence refresh review takes hours. A finding on stale evidence takes weeks of mitigation, regulatory engagement, and documentation.

6 Cross-Standard Evidence Reconciliation

CIP standards interlock. Evidence supporting one standard has to align with evidence supporting the related ones, and an inconsistency can produce findings on several standards at once.

6.1 How the Standards Connect

The CIP standards don't operate independently. The CIP-002 categorization decides which systems every other standard reaches. CIP-005-7 Part 1.1 requires every applicable Cyber Asset connected by a routable protocol to reside within a defined Electronic Security Perimeter. CIP-010-4 Part 1.1 requires a baseline for each applicable system that includes, among other items, the logical network accessible ports and any security patches applied, so the baseline has to agree with the ports and patch records kept under CIP-007-6. When an asset leaves service, CIP-011-3 Requirement R2 requires action to prevent unauthorized retrieval of BES Cyber System Information before it is reused or disposed of.

6.2 What Inconsistency Looks Like

Cross-standard inconsistency is one of the more expensive ways to fail an audit. A system categorized as medium impact under CIP-002 doesn't appear in the CIP-005 perimeter list. A patch shows up in CIP-007 installation records but not in the CIP-010 baseline. A Cyber Asset on the ESP list isn't reflected in the categorization records.

NERC's 2025 annual report shows how far one identification gap can travel. The current CIP standards have no requirement to identify Physical Access Control Systems, Protected Cyber Assets, or Electronic Access Control or Monitoring Systems, yet failing to identify one can break multiple CIP requirements. The ERO Enterprise practice is to process that failure as a single violation under CIP-010 R1, with every other missed requirement documented in the violation description and mitigated. NERC calls this a temporary practice pending a standards fix, and the Standards Committee authorized drafting under Project 2021-03 on October 15, 2025.

6.3 One Authoritative Asset Inventory

Programs that keep their evidence reconciled share one practice: a single, authoritative asset inventory that every CIP standard references. It holds every Cyber Asset, every categorization, every perimeter assignment, and every baseline reference. Updates flow through the inventory, not around it, and evidence captured for any standard is anchored to an inventory entry. A clean inventory also fills the ERT detail tabs with numbers that agree with each other.

It is the foundation that makes large CIP programs auditable at scale. Without it, every audit turns into a forensic reconciliation of separate evidence streams.

7 Common Evidence Failures and What They Cost

The evidence failure patterns repeat. Knowing them in advance is most of the prevention.

7.1 What the Enforcement Data Shows

NERC publishes where CIP noncompliance concentrates. Its ORCP and CMEP Annual Report, issued February 11, 2026, lists the ten CIP standards with the most noncompliance reported in 2025, led by CIP-010, CIP-007, and CIP-004, which the report says "all involve high volume and high frequency conduct." Enforcement cause codes on those filings point to lack of or deficient policies and procedures as the leading root cause for all three. I'd group most evidence failures into a handful of categories, and programs that prepare for those categories avoid most of the findings other programs accept.

7.2 Five Patterns

Pattern one: missing evidence for required controls. The control was implemented. The evidence was never captured, was deleted, or wasn't kept. The audit team finds the gap.

Pattern two: evidence that doesn't match the control description. The evidence shows the control was executed differently from the documented procedure. The auditor records both versions. The finding can run against the procedure, because it didn't reflect operations, or against the control, because it didn't follow the procedure.

Pattern three: evidence with provenance gaps. The auditor can't tell where the evidence came from, who captured it, or whether it's authentic. A provenance gap rarely stays with one artifact. It raises questions about the integrity of the program's evidence as a whole.

Pattern four: evidence that doesn't reconcile across related artifacts. Logs that don't match procedures that don't match attestations. The cross-references break, and the auditor can't reconstruct what actually happened.

Pattern five: stale evidence that no longer reflects current operations. Chapter 5 covered the mechanics. In my view, it is the most common single failure mode in CIP evidence.

Each pattern has its own prevention strategy, and programs that work through the patterns one at a time get better audit outcomes than programs that prepare generically.

> **From the Field**
>
> Generic audit preparation produces generic results. Prepare for the five patterns one at a time.

8 Building an Evidence Program That Survives Audit

In my view, the CIP evidence programs that get through audits without surprises share five characteristics. None are exotic. All require sustained discipline.

8.1 Five Principles

Principle one: evidence is captured as part of the operation, not after it. Every control execution produces evidence as a byproduct. Evidence by design, not evidence by assembly.

Principle two: evidence is inventoried. The program knows what evidence exists, where it's stored, who maintains it, how long it's kept, and which requirements it supports.

Principle three: evidence reconciles across standards. A single authoritative asset inventory anchors the evidence for every CIP standard. The relationships between standards are explicit and checked.

Principle four: evidence is refreshed on a cadence and on change. Periodic re-validation catches drift. Change-triggered refresh catches obsolescence.

Principle five: evidence is audited internally before the external audit arrives. The program draws its own samples, finds its own gaps, and fixes its own issues before the Region does.

8.2 Where the Standards Already Point

Principle	Where the current standards already push it
Capture during operation	CIP-007-6 Part 4.4 (high impact) lists dated documentation of each log review as example evidence
Inventory	CIP-005-7 Part 1.1 measures suggest a list of every ESP and the Cyber Assets in it
Reconcile across standards	CIP-010-4 Part 1.1 baselines include security patches applied
Refresh on change	CIP-010-4 Part 1.3 requires baseline updates within 30 calendar days
Audit internally first	ERT Level 1 populations become the audit team's sample pool

8.3 Design Choices, Not a Checklist

In my view, programs that operate under these five principles spend less on audit defense, produce fewer findings, mitigate faster when findings do occur, and present better to the Region during ongoing oversight. They are program design choices, made early and reinforced for years.

Glossary

Terms marked NERC Glossary are quoted from the Glossary of Terms Used in NERC Reliability Standards as currently enforceable. Several CIP definitions change on July 1, 2028 under the virtualization standards.

Term	Meaning in this paper
Audit period	The period a Compliance Audit covers. Under Appendix 4C of the NERC Rules of Procedure, it begins the day after the End Date of the prior Compliance Audit, and the entity's data must show compliance for the entire period.
BES Cyber System	One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity. (NERC Glossary)
BES Cyber System Information (BCSI)	Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. (NERC Glossary, first sentence)
CIP Evidence Request Tool (ERT)	The common request for information the Regional Entities use for CIP audits. Level 1 collects populations and program documents; Level 2 requests implementation evidence for sampled items.
Compliance Enforcement Authority (CEA)	NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards, as defined in the NERC Rules of Procedure.
Cyber Assets	Programmable electronic devices, including the hardware, software, and data in those devices. (NERC Glossary)
Electronic Access Control or Monitoring Systems (EACMS)	Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems. (NERC Glossary)
Electronic Security Perimeter (ESP)	The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol. (NERC Glossary)
Physical Access Control Systems (PACS)	Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers. (NERC Glossary)
Protected Cyber Assets (PCA)	One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. (NERC Glossary, first sentence)

How Energy Compliance Can Help

EC partners with registered entities on the institutional and technical questions that define strong reliability and cybersecurity programs, from classification through audit through enforcement response. Our services are written to be operationally executable in real time and audit-defensible at compliance review. A senior practitioner oversees every engagement.

Evidence and audit readiness. Regulator-perspective program reviews that test a CIP evidence program the way an audit team will. Audit and enforcement support (non-advocacy); audit defense with Notice of Penalty response and settlement posture; RSAW production and data request strategy; NERC compliance program support, interpretation, and audit preparation. Where an evidence trail needs its provenance checked, an Evidence Provenance Review.

Program design. Compliance program design and improvement; reliability governance and program assessments; registration and applicability analysis; mitigation planning and Self-Report development; operational and engineering reliability alignment.

Advisory and training. NERC reliability and compliance advisory support; senior advisory on complex reliability questions; training and executive briefings on reliability frameworks; industry engagement in standards development and working-group participation.

Each engagement is scoped to the entity's role, function, and bulk system impact.

WattOps Compliance is EC's NERC compliance evidence platform (wattopscompliance.com). It applies the same evidence discipline to the non-CIP standards your CIP team doesn't own. 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, the operations data behind a compliance position deserves the same provenance as the CIP evidence.

Pull your last Level 1 populations and sample them yourself. If the evidence for any row is hard to find, 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), Rules of Procedure, Appendix 4C, Compliance Monitoring and Enforcement Program (effective May 19, 2022). https://www.nerc.com/globalassets/who-we-are/rules-of-procedure/appendix-4c.pdf
- NERC, Critical Infrastructure Protection Evidence Request Tool User Guide (January 2026). https://www.nerc.com/globalassets/programs/compliance/cmep-resources/cip-evidence-request-tool-user-guide-v10.pdf
- NERC, 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, 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-005-7, Cyber Security: Electronic Security Perimeter(s). https://www.nerc.com/globalassets/standards/reliability-standards/cip/cip-005-7.pdf
- NERC, Reliability Standard CIP-007-6, Cyber Security: System Security Management. https://www.nerc.com/globalassets/standards/reliability-standards/cip/cip-007-6.pdf
- NERC, Reliability Standard CIP-010-4, Cyber Security: Configuration Change Management and Vulnerability Assessments. https://www.nerc.com/globalassets/standards/reliability-standards/cip/cip-010-4.pdf
- NERC, Reliability Standard CIP-011-3, Cyber Security: Information Protection. https://www.nerc.com/globalassets/standards/reliability-standards/cip/cip-011-3.pdf
- NERC, Reliability Standards: CIP standards listing with status and effective dates (CIP-003-9, CIP-012-2, the 2028 virtualization set, CIP-002-8, CIP-015-1). https://www.nerc.com/standards/reliability-standards/cip
- NERC, Glossary of Terms Used in NERC Reliability Standards. https://www.nerc.com/glossary-of-terms
- 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 Fed. Reg. 14013 (March 24, 2026), FR Doc. 2026-05715. https://www.govinfo.gov/content/pkg/FR-2026-03-24/pdf/2026-05715.pdf

© Energy Compliance, Inc. · EC-WP-207 · October 2026