FOUNDATIONS SERIES · EC-WP-104

NERC Compliance Monitoring and Enforcement Explained

How CMEP turns mandatory standards into actual compliance pressure

Your last clean audit doesn't mean you have a good compliance program. It might mean the Regional Entity hasn't looked at the right thing yet. CMEP, end to end.

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, engineering advice, or formal interpretation of any NERC Reliability Standard, FERC order, RTO or ISO protocol, or state commission rule.

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

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

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

Foreword

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

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

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

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

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

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

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

CMEP is the gear that turns mandatory standards into actual compliance pressure. The Compliance Monitoring and Enforcement Program, Appendix 4C to the NERC Rules of Procedure, is how NERC and the Regional Entities determine whether registered entities are doing what the standards require, and what happens when they are not. Every Generator Owner, Transmission Operator, Reliability Coordinator, Balancing Authority and Distribution Provider operates inside this framework, whether they think about it daily or only when an audit notice arrives.

This reference walks CMEP end to end, from the statute and the roles of FERC, NERC and the Regional Entities through monitoring, enforcement, mitigation, penalties and due process.

Seven points carry through every chapter:

- Your last clean audit doesn't mean you have a good compliance program. It might mean the Region hasn't looked at the right thing yet. Audit scope is tailored to your risk profile, and the obligation covers every applicable standard, audited or not.
- Appendix 4C lists seven compliance monitoring processes plus Self-Logging. Each carries a different procedural footprint and notice period. Knowing which one is happening to you on a given day is the difference between preparation and reaction.
- Self-Reports are the cheapest violations to mitigate. Audit findings are the most expensive. The difference is who found it first, and an audit notification letter generally ends self-reporting credit for the requirements in scope.
- Risk-based oversight isn't random. Knowing what makes you a higher-risk target lets you reduce the target.
- Mitigation that addresses symptom and ignores cause buys you the same finding next cycle. Appendix 4C requires a Mitigation Plan to correct the cause and prevent recurrence, not just fix the instance.
- Penalties scale to risk and to behavior, not to paperwork. The same finding produces different penalties depending on what you did before, during, and after.
- Most noncompliance never reaches a penalty. In 2025, the ERO Enterprise resolved about 83 percent of filed or submitted noncompliance as Compliance Exceptions and about 14 percent through Find, Fix, Track and Report.

The chapters cite the Federal Power Act, FERC's regulations, and the NERC Rules of Procedure and their appendices directly. Where a statement is my judgment rather than a rule, the text says so.

1 Purpose of Compliance Monitoring and Enforcement

1.1 What CMEP Is

The Compliance Monitoring and Enforcement Program is the program NERC and the Regional Entities use to monitor, assess and enforce compliance with Reliability Standards in the United States. Appendix 4C says so in its first sentence, and it adds that the program is also implemented in Canada and Mexico consistent with the laws and agreements in effect with the governmental authorities there.

Section 401 of the NERC Rules of Procedure sets the mandate. NERC must develop and implement a CMEP to promote the reliability of the Bulk Power System by enforcing compliance with approved Reliability Standards wherever NERC or a Regional Entity has been given enforcement authority. The same section states who must comply: where legislation, regulation, rule or agreement requires it, all Bulk Power System owners, operators and users must comply with all approved Reliability Standards at all times.

1.2 Where the Authority Comes From

The authority is statutory. The Energy Policy Act of 2005 added Section 215 to the Federal Power Act. Section 215(e) lets the Electric Reliability Organization impose a penalty on a user, owner or operator of the bulk-power system for violating a FERC-approved standard, but only after notice and an opportunity for a hearing, and only after it files the notice and the record of the proceeding with FERC.

FERC's regulations build the machinery underneath. Under 18 C.F.R. § 39.7(a), the ERO and each Regional Entity must have an audit program that provides for rigorous audits of compliance. Section 39.7(b) requires procedures to report promptly to FERC any self-reported violation, any investigation, and any alleged violation, along with its eventual disposition.

Before mandatory standards, the rules had no teeth. In Order No. 693, FERC recounted that the August 14, 2003 blackout affected an estimated 50 million people and 61,800 megawatts of load, and that a joint U.S.-Canada task force found it was caused by several entities violating NERC's then-effective policies and standards. CMEP is the answer to that finding. A standard nobody verifies is a suggestion.

1.3 Two Halves of One System

The standards tell you what's required. CMEP tells you whether you actually did it. The framework only works because both halves exist.

The monitoring half is the set of processes in Section 4.0 of Appendix 4C: Compliance Audits, Self-Certifications, Spot Checks, Compliance Investigations, Self-Reports, Self-Logging, Periodic Data Submittals and Complaints. The enforcement half is Sections 4A through 7.0: the streamlined dispositions, enforcement actions, mitigation and Remedial Action Directives. The Sanction Guidelines in Appendix 4B set the penalty method.

Two rules connect the halves. First, every Bulk Power System owner, operator and user must provide NERC or the Compliance Enforcement Authority with the documents, data and information needed to monitor and enforce compliance (Rules of Procedure Section 401.3). Second, paying a penalty does not buy an exemption. Appendix 4C states that the imposition and acceptance of penalties and sanctions shall not be considered an acceptable alternative to an entity's continuing obligation to comply.

1.4 Accountability With Due Process

CMEP is built to hold entities accountable and to treat them fairly while doing it. The statute requires notice and an opportunity for a hearing before a penalty. It requires that any penalty bear a reasonable relation to the seriousness of the violation and take into account the entity's efforts to remedy it in a timely manner (FPA Section 215(e)(6)). Every penalty the ERO files is subject to FERC review.

The program is also designed to put effort where the risk is. Appendix 4C directs the Compliance Enforcement Authority to set the type and frequency of monitoring based on the entity's specific risks to the Bulk Power System, and it lets noncompliance that poses no serious or substantial risk be resolved through streamlined processes. That design choice runs through every chapter that follows.

1.5 Compliance Is Not Reliability

In my view, the most common mistake in this business is treating CMEP as the goal. It isn't. CMEP exists to verify a minimum level of reliability performance. A program built only around what gets audited will pass audits and still miss risk. Build the program around how the system can fail, and the audit evidence follows.

End-of-Chapter Summary

CMEP is the statutory enforcement arm of the Reliability Standards. It rests on FPA Section 215, FERC's Part 39 regulations, and the NERC Rules of Procedure, and it is carried out through Appendix 4C. It pairs monitoring with enforcement, guarantees notice and a hearing before any penalty, and scales oversight to risk. Penalties never replace the obligation to comply.

> **From the Field**
>
> CMEP isn't paperwork. It's the mechanism that turns "you should comply" into "you have to." If your compliance program is built around what gets audited, you've already missed the point. CMEP exists to verify reliability. Reliability is the goal. Audit is just the lens.

2 Roles of NERC, Regional Entities, and FERC in Oversight

2.1 FERC: The Regulator Above the ERO

Section 215 gives FERC jurisdiction over the ERO, the Regional Entities, and all users, owners and operators of the bulk-power system. FERC certified NERC as the ERO in 2006 (116 FERC ¶ 61,062). Within the compliance framework, FERC holds five powers that matter most to a registered entity:

- It approves Reliability Standards, and on its own motion or on complaint it can order the ERO to submit a new or modified standard that addresses a specific matter (FPA Section 215(d)(5)).
- It can review any penalty. A penalty the ERO imposes cannot take effect earlier than the 31st day after the notice of penalty is filed, and FERC can review it on its own motion or on the entity's application (FPA Section 215(e)(2)).
- It can enforce directly. On its own motion or on complaint, FERC can order compliance with a standard and impose a penalty after notice and an opportunity for a hearing (FPA Section 215(e)(3)).
- It can investigate on its own authority. Investigations FERC initiates run under FERC's own statutory authority and rules, not the Appendix 4C procedures (Appendix 4C, Section 4.4).
- It can direct an unscheduled Compliance Audit. Appendix 4C requires the Compliance Enforcement Authority to initiate one if FERC directs it (Section 4.1.2).

The Energy Policy Act also settled what the ERO and the Regional Entities are not. Section 1211(b) of the Act provides that the certified ERO and any Regional Entity with delegated enforcement authority are not departments, agencies or instrumentalities of the United States Government.

2.2 NERC: Program Owner and Consistency Check

NERC owns the program. It develops and implements CMEP under Section 401, oversees how the Regional Entities carry it out under Section 402, and identifies the risk elements that drive annual oversight priorities under Section 401.6.

NERC's enforcement role is concrete. It reviews and approves every settlement for consistency with settlements of similar violations. It receives each notification of Confirmed Violation, can send it back for more factual development, and prepares and files the Notice of Penalty with FERC. It can direct a Regional Entity to revise a penalty determination. Appendix 4C states that NERC works to achieve consistency in the application of the Sanction Guidelines across Regional Entities through direct oversight and review of penalties and sanctions.

NERC can also step in. It reserves the right to lead a Compliance Investigation, for example to keep investigative processes consistent, to coordinate a matter that crosses Regional Entity boundaries, or where a Regional Entity cannot conduct the investigation. The Regional Entity cannot appeal that decision.

2.3 Regional Entities: Day-to-Day Monitoring and Enforcement

Section 215(e)(4) of the Federal Power Act authorizes the ERO to delegate enforcement authority to a regional entity through an agreement FERC approves. There are six Regional Entities: Midwest Reliability Organization (MRO), Northeast Power Coordinating Council (NPCC), ReliabilityFirst (RF), SERC Reliability Corporation (SERC), Texas Reliability Entity (Texas RE) and WECC. Together with NERC they make up the ERO Enterprise.

Each Regional Entity with a delegation agreement administers CMEP for its footprint (Rules of Procedure Section 401.4). When it does, it acts as the Compliance Enforcement Authority, or CEA, the term Appendix 2 uses for NERC or the Regional Entity in its role of monitoring and enforcing compliance. The CEA runs the audits and spot checks, requests Self-Certifications and data, reviews Self-Reports, conducts investigations, performs Preliminary Screens, accepts or rejects Mitigation Plans, and negotiates settlements.

Regional Entities also do outreach. NERC's 2025 annual report records that the six Regional Entities hosted dozens of workshops and training events for industry in the United States and Canada that year.

2.4 One Violation, One Enforcement Action

The structure protects entities from double jeopardy. Under Rules of Procedure Section 401.8, a registered entity cannot be subject to an enforcement action by both NERC and a Regional Entity, or by more than one Regional Entity, for the same violation, unless it is registered in more than one Region in which the violation occurred.

The layering also gives every enforcement action at least two sets of eyes beyond the auditor. The Regional Entity decides. NERC reviews for consistency and files. FERC can review, modify or set aside. In my view, that layering is where consistency comes from. It is also why an entity that thinks its Regional Entity got it wrong has somewhere to go.

End-of-Chapter Summary

FERC certifies the ERO, approves the standards, can review any penalty and can enforce on its own. NERC owns CMEP, sets the risk priorities, approves settlements and files Notices of Penalty. The six Regional Entities do the day-to-day monitoring and enforcement under delegation agreements FERC approves. An entity faces one enforcement action per violation.

3 Risk-Based Oversight Philosophy and Reliability Impact

3.1 Risk Decides Where Oversight Lands

Risk-based oversight is written into the program, not layered on top of it. Appendix 4C directs the CEA to determine the type and frequency of compliance monitoring based on the registered entity's specific risks to the reliability of the Bulk Power System. Rather than applying the same scrutiny to every requirement at every entity, the ERO Enterprise decides where to look based on what could hurt the system.

That choice does not shrink the obligation. Rules of Procedure Section 401.6 states plainly that compliance is required with all applicable Reliability Standards, and that NERC and the Regional Entities have authority to monitor all of them, whether or not they are identified as focus areas in the annual implementation plan or in a Regional Entity's oversight plan for the entity. Risk changes the order in which things get checked. It does not change what has to be true.

3.2 Risk Elements and the ERO CMEP Implementation Plan

At the continent-wide level, risk is set through the ERO CMEP Implementation Plan. NERC, with input from the Regional Entities, stakeholders and regulators, identifies risk elements and the related standards and requirements to prioritize for oversight. Appendix 4C lists the data NERC considers: emerging risks, compliance findings, event analysis experience, data analysis, and the expert judgment of NERC and Regional Entity staff, committees and subcommittees.

NERC posts the plan on its website on or about November 1 of the year before it is implemented. NERC and the Regional Entities can update it during the year to reflect changing risk. Read it every fall. It is the closest thing to a published list of what the auditors will care about next year.

3.3 Inherent Risk Assessments and Compliance Oversight Plans

At the entity level, risk is set through the Inherent Risk Assessment. Appendix 2 defines an IRA as the CEA's review of the potential risks an individual registered entity poses to the reliability of the Bulk Power System. It considers factors such as assets, system, geography, interconnectivity, prior compliance history and factors unique to the entity. The results can put more, fewer or different standards in scope for that entity than the implementation plan identifies.

Alongside the IRA sits the Compliance Oversight Plan, or COP. NERC's 2025 annual report describes the ERO Enterprise's Align system as supporting both, and the report charts IRA and COP completion against the audits planned for each period. For audits, Appendix 4C ties scope

directly to this work: the CEA tailors the scope of a Compliance Audit to the standards identified through the NERC-approved risk-based processes, including IRAs, internal controls and other inputs.

That is why risk-based oversight isn't random. Several of the IRA inputs, such as compliance history and the quality of internal controls, are things an entity can change. Knowing what makes you a higher-risk target lets you reduce the target.

3.4 Violation Risk Factors, Severity Levels and Time Horizons

Each requirement carries its own risk weighting, set before any violation occurs. The Sanction Guidelines explain the three tools:

- **Violation Risk Factor (VRF).** Assigned to every requirement through the standards development process, at one of three levels: Lower, Medium or High. It reflects the expected or potential impact of a violation on the reliability of the Bulk Power System.
- **Violation Severity Level (VSL).** Assessed after a violation, at one of four levels: Lower, Moderate, High or Severe. It measures how far short the entity fell.
- **Violation Time Horizon.** The operating time frame the requirement addresses. In general, violations of requirements with shorter horizons, such as Real-time Operations, carry a higher penalty multiplier than those with longer horizons, such as Long-term Planning.

Then comes the assessed risk of the actual violation: minimal, moderate, or serious and substantial. The Sanction Guidelines define assessed risk as the potential impact to reliability multiplied by the likelihood of that impact occurring, or the actual harm if it did occur, based on facts about the entity and the scope of the violation. A High VRF requirement violated at a small facility under conditions where nothing could go wrong may still be minimal risk. The facts decide.

3.5 How Risk Shapes the Outcome

Assessed risk drives disposition. Appendix 4C reserves the Compliance Exception process for minimal-risk noncompliance and the Find, Fix, Track and Report (FFT) process for minimal or moderate risk. Noncompliance that does not fit either goes through the enforcement process in Section 5.0. Chapter 7 walks those paths.

In my view, this is where entities lose the most ground without knowing it. The risk assessment in your Self-Report or your response to a Preliminary Screen is your first chance to frame the facts. Write it with the same care you would put into a hearing brief.

End-of-Chapter Summary

Risk sets the type and frequency of monitoring, the scope of each audit, and the disposition of each noncompliance. Continent-wide risk elements come through the annual ERO CMEP Implementation Plan. Entity-level risk comes through the Inherent Risk Assessment and the Compliance Oversight Plan. VRFs, VSLs, time horizons and assessed risk weight each violation. None of it narrows the obligation to comply with every applicable standard.

4 Compliance Monitoring Methods and Tools

4.1 The Monitoring Processes

Appendix 4C, Section 4.0, sets out seven compliance monitoring processes and a Self-Logging alternative to Self-Reports. Each has its own trigger and its own notice period.

Process	Who starts it	Notice to the entity (Appendix 4C)
Compliance Audit	CEA, on a risk-based schedule or unscheduled	Intent to audit at least 270 days ahead; audit notice and data request at least 90 days ahead; at least 10 business days for an unscheduled audit (Sec. 4.1)
Self-Certification	CEA request	Request at least 60 days in advance (Sec. 4.2)
Spot Check	CEA discretion or NERC direction	Notification letter with reason and scope; at least 20 days to submit (Sec. 4.3)
Compliance Investigation	CEA, after a disturbance, Complaint or other indication	Notice of initiation and initial scope within 3 business days of the decision (Sec. 4.4)
Self-Report	Registered entity	Encouraged when the entity becomes aware it has or may have violated a standard (Sec. 4.5)
Self-Logging	Approved registered entity	Log of minimal-risk noncompliance, reviewed by the CEA at least every 3 months (Sec. 4.5A)
Periodic Data Submittal	Schedule in the standard or set by the CEA	The standard's notice period; otherwise normally no less than 20 days (Sec. 4.6)
Complaint	Anyone, including anonymously	CEA notifies NERC and reviews for sufficient basis (Sec. 4.7)

4.2 Risk Sets the Mix

The CEA chooses which process to apply, and how often, based on the entity's specific risks. In practice, most monitoring happens on paper. NERC's 2025 annual report counted 1,214 Self-Certifications, 134 audits and 47 spot checks across the ERO Enterprise that year. Self-Certifications made up about 87 percent of compliance monitoring engagements, with audits and spot checks about 13 percent.

That ratio should change how you think about preparation. The audit is the visible event, but the Self-Certification is the engagement you will face most often, and it carries a signature.

4.3 Data Requests and Signatures

Every monitoring process runs on documents, data and information. Appendix 4C gives the CEA authority to collect them in the manner it deems most appropriate, including requesting copies and removing those copies from the entity's location under security procedures conforming to Section 1500 of the Rules of Procedure. If requested material does not arrive by the Required Date, the CEA can execute the steps in Attachment 1, Process for Non-submittal of Requested Data.

Two protections and one obligation are worth knowing:

- If an entity believes a request for documents, data or information is unreasonable, it can ask the NERC general counsel for a written determination.
- Receipt of a Self-Certification or a Periodic Data Submittal is not a finding that the entity is compliant or noncompliant (Sections 4.2.1 and 4.6.1).
- Any report or submission CMEP requires must be signed by an officer, employee, attorney or other authorized representative of the entity, and NERC or the CEA can ask the signer to state the basis of that authority.

4.4 How the Processes Feed Each Other

The processes are not separate tracks. A Complaint can lead to a spot check or an investigation. A spot check can test a Self-Certification, a Self-Report or a Periodic Data Submittal, or follow a system event; Appendix 2 defines it that way. A failed Mitigation Plan can draw a Compliance Audit or a Remedial Action Directive (Section 6.6).

Whatever the source, every potential noncompliance ends up in the same place. When any monitoring process, or any other means, turns up information indicating a potential noncompliance, the CEA must conduct a Preliminary Screen within ten business days (Section 4.8). Chapter 7 picks up from there.

End-of-Chapter Summary

CMEP monitors through Compliance Audits, Self-Certifications, Spot Checks, Compliance Investigations, Self-Reports, Self-Logging, Periodic Data Submittals and Complaints. Each has a defined trigger and notice period. Risk sets the mix, and in 2025 Self-Certifications made up about 87 percent of engagements. Every potential noncompliance, however found, goes to a Preliminary Screen within ten business days.

5 Audits and Spot Checks Explained

5.1 What a Compliance Audit Is

Appendix 2 defines a Compliance Audit as a systematic, objective review and examination of records and activities to determine whether a registered entity meets the requirements of applicable Reliability Standards. All registered entities are subject to audit for the standards that apply to the functions for which they are registered. Audits may be conducted on site at the CEA's discretion.

Audits follow professional auditing standards. For audits in the United States, Appendix 4C bases the process on professional auditing standards recognized in the United States, which may include Generally Accepted Auditing Standards, Generally Accepted Government Auditing Standards, and standards sanctioned by the Institute of Internal Auditors. NERC posts Compliance Guidance documents and Reliability Standard Audit Worksheets (RSAWs) on its website. Read the RSAW before you build the evidence, not after.

5.2 The Audit Timeline

Section 4.1.1 lays out the sequence:

1. At least 270 days before a planned audit, the CEA notifies the entity that it plans to audit it.
2. At least 90 days before the audit, the CEA sends the audit notice: the standards to be evaluated, the audit team members and their recent employment history, and the request for documents, data and information.
3. The entity provides the material in the format and by the Required Date in the request.
4. The audit team reviews it against the requirements.
5. The team holds an exit briefing, gives the entity a chance to review the audit report before it is final, and completes the report.

The entity can object to any audit team member for a conflict of interest or other circumstances that could interfere with impartial performance. Objections are due in writing no later than 30 days before the audit starts, or within five business days of notice for a member appointed less than 35 days before the start. For an unscheduled audit, objections are due at least five business days before on-site work begins. The CEA makes the final call.

The CEA can also launch an unscheduled audit at any time if it reasonably determines one is necessary, with at least ten business days' notice that names the audit team. It must do so if FERC directs it.

5.3 The Audit Period

The entity must show compliance for the entire audit period. That period begins the day after the End Date of the prior Compliance Audit by the CEA. For an entity never audited before, it begins

on the later of June 18, 2007 or the date the entity became subject to the standards. The End Date is set before the audit starts, for example the date of the audit notification or 30 days after it.

One rule protects entities with short retention periods. If a standard's retention period does not cover the whole audit period, the entity will not be found in noncompliance solely for lacking information it rightfully did not retain. The CEA will require the entity to demonstrate compliance through other means.

5.4 The Audit Report

The draft audit report describes the objective, scope and methodology. It identifies any evidence of potential noncompliance and any Remedial Action Directives, Mitigation Plans or other Mitigating Activities reviewed. It may also state areas of concern and recommendations. The entity has 30 days to comment on the draft and to identify Confidential Information it proposes for redaction.

The final report goes to NERC, and NERC sends it to FERC where FERC has jurisdiction. NERC will not publicly post a final audit report for at least five business days after receipt. If the report identifies potential noncompliance, the part identifying it stays non-public until final disposition: dismissal, or NERC's submission of a disposition to FERC. Confidential Information is redacted from any public report.

5.5 Spot Checks

A spot check is narrower and faster. Appendix 2 defines it as a process in which the CEA requests information to support the entity's Self-Certification, Self-Report or Periodic Data Submittal and assess compliance; as a random check; or in response to operating problems or system events. The CEA can start one at its discretion or at NERC's direction.

Section 4.3.1 sets the process:

- A notification letter states that a spot check will be performed, the reason for it, and its scope, including the requirements covered. The entity gets at least 20 days to submit or make material available.
- The notification package names the spot check team and gives their recent employment histories. Objections follow the audit grounds and are due by the later of five business days before the material is submitted or five business days after the entity learns who is on the team.
- The spot check may require document submission and an on-site review.
- The team prepares a draft report and gives the entity ten business days to comment.
- The final report goes to the entity and NERC, and through NERC to FERC where FERC has jurisdiction. Unlike an audit report, a spot check report is not publicly posted by the CEA or NERC.

5.6 What an Audit Does and Does Not Tell You

An audit answers one question: did the evidence show that the requirements in scope were met for the audit period? It does not grade the operational quality of the organization, and it does not cover standards that were out of scope.

That is the point behind the line at the top of this reference. Audit scope is tailored by the IRA, the internal controls review and other inputs, and the scope may include standards whether or not they appear in the implementation plan. A clean audit means the auditors did not find noncompliance in what they looked at. In my view, the program that treats a clean audit as a verdict on everything is the program most likely to be surprised by the next one.

End-of-Chapter Summary

A Compliance Audit is a systematic review of records and activities over a defined audit period, conducted under recognized auditing standards with 270-day and 90-day notices, team objection rights, an exit briefing and a 30-day comment period on the draft report. A spot check is a narrower review with at least 20 days to respond, ten business days to comment, and no public posting. Neither tells you more than what was in scope.

> **From the Field**
>
> Your last clean audit doesn't mean you have a good compliance program. It might mean the Region hasn't looked at the right thing yet.

6 Self-Reporting, Self-Certifications, and Event-Based Reviews

6.1 Self-Reports

Appendix 4C encourages Self-Reports at the time an entity becomes aware that it has, or may have, violated a standard. The content requirements are specific. A Self-Report includes:

- a risk assessment of the noncompliance,
- a description of its extent,
- its cause, and
- the actions taken or planned to mitigate it, including preventing recurrence.

The CEA reviews the Self-Report and may ask for clarification or more information. Notice what the list asks for. It is the same structure as a Mitigation Plan. An entity that writes a strong Self-Report has already done half the mitigation work.

6.2 Why Self-Reports Are the Cheapest Violations

The Sanction Guidelines make self-reporting a mitigating factor. NERC or the Regional Entity considers whether the entity self-reported within a reasonably prompt time after becoming aware of the violation, and before detection through a compliance monitoring engagement or a notification of an upcoming one. The guidelines say an entity should submit a Self-Report as soon as practical, but typically within three months of discovery.

The timing rule has a hard edge. A notification letter for an upcoming audit, spot check or Self-Certification that lists the requirements in scope generally ends the entity's eligibility for self-reporting credit on those requirements until the engagement is over. If you suspect a problem in a requirement that might be in next year's audit scope, the time to report it is before the 90-day letter arrives.

The ERO Enterprise reads self-reporting as a sign of health. NERC's 2025 annual report states that it looks for high levels of self-reported noncompliance as an indicator of good detective controls and strong compliance cultures, and it reports that about 85 percent of reported noncompliance in 2025, and about 85 percent over the past five years, was self-identified by registered entities.

6.3 Self-Logging

Self-Logging is the step beyond Self-Reports for entities with mature controls. Under Section 4.5A, an entity found eligible by the CEA after a formal review of its internal controls can be approved to log noncompliance for later review instead of submitting individual Self-Reports. The rules:

- The log is limited to noncompliance posing a minimal risk, unless a governmental authority authorizes otherwise.
- Each entry carries a detailed description, the risk assessment, and the Mitigating Activities completed or planned.
- There is a rebuttable presumption that logged noncompliance will be resolved as a Compliance Exception.
- The CEA reviews the logs at least every three months, with a possible extension to six, and NERC and governmental authorities can review them on request.

6.4 Self-Certifications

A Self-Certification is an attestation. Appendix 2 defines it as an entity's attestation that it is compliant or noncompliant with the requirement, that it does not own Facilities subject to the requirement, or that the requirement does not apply to it. The CEA requests it at least 60 days in advance and specifies the information it wants.

At a minimum, the CEA reviews Self-Certifications of noncompliance and those claiming no applicable Facilities or no applicability. It can ask for more. Receipt of a Self-Certification is not a finding of compliance, noncompliance or applicability. In my view, an entity should treat every Self-Certification as signed testimony, because it is a signed CMEP submission and the CEA can test it with a spot check.

6.5 Event-Based Reviews

Appendix 4C does not create a separate monitoring process called an event-based review. Events reach CMEP through the processes that already exist. A Compliance Investigation may be initiated in response to a system disturbance (Section 4.4). A spot check may be conducted in response to operating problems or system events (Appendix 2). A system event can also prompt a Complaint or a Self-Report.

Event analysis itself sits elsewhere in the Rules of Procedure. Section 800 covers reliability assessment and performance analysis, and Section 807 sets NERC's role after major events such as significant losses of load or generation or significant disturbances.

The practical point holds either way. A reliability event does not necessarily mean noncompliance, and noncompliance does not necessarily mean an event. After an event, expect the questions to come from both directions.

End-of-Chapter Summary

Prompt Self-Reports filed before a monitoring notice earn mitigating credit. Self-Logging carries a presumption of Compliance Exception treatment. Self-Certifications are signed attestations, not findings. Events enter CMEP through existing processes.

> **From the Field**
>
> Self-Reports are the cheapest violations to mitigate. Audit findings are the most expensive. The difference is who found it first.

7 Investigation and Enforcement Process

7.1 Compliance Investigations

In my view, a Compliance Investigation is the most intrusive monitoring process. Appendix 2 defines it as a comprehensive investigation, which may include an on-site visit with interviews, to determine whether a violation has occurred. The CEA can start one at any time in response to a system disturbance, a Complaint, or any potential noncompliance identified by other means. Regional Entity staff generally lead it, and NERC can take over.

Investigations are confidential unless FERC directs otherwise. The process under Section 4.4.1:

- Within three business days of deciding to investigate, the CEA notifies the entity of the initiation and initial scope, instructs it to preserve all relevant records and information, and copies NERC. The scope can expand as facts develop.
- NERC assigns a staff member to the investigation and notifies FERC within three business days.
- The CEA requests documents, data and information and names the team. Within ten business days of the notification, the entity can object to individual team members for conflict of interest, but not to participation by NERC, FERC staff, or staff of another governmental authority with reliability jurisdiction.
- The CEA can require a verification under oath of the entity's responses and can require officers or employees familiar with the matter to be interviewed or testify under oath. Counsel for the person being interviewed may be present.
- If the CEA finds no violation, it notifies the entity and NERC that the investigation is complete.

7.2 The Preliminary Screen

Every path into enforcement starts with a Preliminary Screen. Within ten business days after a potential noncompliance is identified, the CEA determines three things:

1. whether the entity allegedly involved is a registered entity;
2. whether the requirement is applicable to the entity, approved by the governmental authority, and in effect at the time; and
3. if known, whether the matter duplicates one already being processed.

If the screen is affirmative, a potential noncompliance exists. The CEA then sends the entity and NERC a notice that identifies the potential noncompliance, describes it briefly with the requirements involved and, if known, the dates, and instructs the entity to retain and preserve all related data and records. NERC notifies FERC within two business days of receiving notice of a potential noncompliance (Section 8.2).

7.3 The Disposition Paths

After the screen, the CEA assesses the facts and decides whether evidence shows a violation or the matter should be dismissed. If there is a violation, the path depends on risk.

Path	Used for	What it involves
Dismissal	No evidence of violation	CEA issues a Notice of Completion of Enforcement Action (Sec. 5.10)
Compliance Exception	Minimal risk	Entity mitigates; facts available to NERC and governmental authorities; entity may object to this treatment; not counted as compliance history for penalty purposes, with limits (Sec. 4A.1)
Find, Fix, Track and Report	Minimal or moderate risk	Entity mitigates; facts available for review; tracked for trends; entity may object (Sec. 4A.2)
Enforcement action	Everything else	Notice of Alleged Violation and Proposed Penalty or Sanction (NAVAPS) or settlement offer, then Confirmed Violation and Notice of Penalty (Sec. 5.3 to 5.9)

Compliance Exceptions have a limit. If an unremediated matter contributes to a later serious or substantial noncompliance, the CEA must consider that history. Neither Compliance Exceptions nor FFTs carry penalties under the Sanction Guidelines.

7.4 The NAVAPS and the Thirty-Day Election

When a Compliance Exception or FFT is not appropriate, the CEA notifies the entity of the Alleged Violation through an offer of settlement or a NAVAPS, delivered electronically and effective on the date of the electronic notice. At a minimum it states the requirement allegedly violated, when the violation occurred, the facts, and the proposed penalty or sanction with its basis.

The entity then has 30 days to elect one of three positions:

1. agree with the violation and the proposed penalty, and agree to submit and implement a Mitigation Plan or other Mitigating Activities;
2. agree with the violation and mitigate, but contest the penalty; or
3. contest both.

Silence is a choice. An entity that does not respond within 30 days is deemed to have accepted the violation and the penalty, and the CEA issues a Notice of Confirmed Violation. An entity that contests files a signed response with its support. The CEA schedules a conference within ten business days. If issues remain unresolved 40 days after the response, the entity may request a hearing; the two sides can agree in writing to extend that period. If no hearing is requested before the 40 days run, the violation becomes a Confirmed Violation.

Submitting Mitigating Activities while contesting does not waive the right to contest. Use that. Mitigation that starts the day you learn of the problem helps the reliability case and the penalty case at the same time.

7.5 Settlement

Either side can open settlement at any time, even before a NAVAPS issues, and either can end it. While the CEA is negotiating, the 30-day response clock is suspended. The CEA can decline to settle once a matter has become a Confirmed Violation.

Section 5.6 sets the terms:

- NERC is notified of all settlement negotiations, may participate, and must approve the result.
- A settlement must not compromise reliability and must waive the entity's right to further hearings and appeal.
- The agreement may say the entity admits the violation, does not contest it, or neither admits nor denies it. It may not say the entity denies it.
- NERC reviews each settlement for consistency with similar cases and approves or rejects it, and can state the changes that would win approval.
- After approval, NERC reports the settlement to FERC and publicly posts information about the violation and the penalty, with a copy or description of the settlement and the mitigation, redacting critical infrastructure and Confidential Information.

7.6 Confirmed Violation to Notice of Penalty

A Confirmed Violation goes to NERC, which uses the record to prepare a Notice of Penalty. NERC files it with FERC no sooner than five business days after it approves the Confirmed Violation or the settlement, and the CEA must tell the entity at least five business days before public filing.

Under Appendix 4C, the penalty becomes effective when the 30-day period after filing expires, or on FERC's final determination if FERC reviews it. The CEA then issues a payment due notice and invoice with a due date 30 days out. When the entity has paid and completed every requirement in the Notice of Penalty and any settlement, the CEA issues a Notice of Completion of Enforcement Action and the matter closes.

7.7 Remedial Action Directives

Some situations cannot wait for the process. Under Section 7.0, the CEA may issue a Remedial Action Directive when action is immediately necessary to protect the Bulk Power System from an imminent or actual threat. A directive can impose limits, studies, testing, training or increased auditing, or require the entity to stop an activity that may violate a standard.

Before issuing one, the CEA must consult the entity's Reliability Coordinator. The entity has two business days after actual receipt to contest it in writing, and the hearing runs on an expedited procedure. Failing to comply with a directive is an aggravating factor under the Sanction Guidelines.

End-of-Chapter Summary

Every potential noncompliance gets a Preliminary Screen, then dismissal, Compliance Exception, FFT or enforcement. A NAVAPS starts a 30-day election; silence is acceptance.

8 Mitigation, Corrective Action, and Risk Reduction

8.1 Mitigation Is Required, and It Is Not an Admission

Every entity found in noncompliance must mitigate it. Under Section 6.1, the entity files a description of how the noncompliance will be or has been mitigated, and the CEA can ask for a formal Mitigation Plan. Appendix 2 draws the distinction: Mitigating Activities are actions to correct and prevent recurrence of a noncompliance, whether or not they are in a Mitigation Plan. A Mitigation Plan is an action plan to correct the noncompliance and prevent it from happening again.

Appendix 4C states that submitting a Mitigation Plan does not constitute an admission of a violation. That rule removes the most common excuse for waiting.

8.2 What a Mitigation Plan Must Contain

Section 6.2 lists the required contents:

- a point of contact who is responsible for the plan, technically knowledgeable and authorized to answer for it;
- the potential noncompliance the plan will correct;
- the cause of the potential noncompliance;
- the Mitigating Activities to correct the noncompliance;
- the Mitigating Activities to correct the cause;
- the Mitigating Activities to prevent recurrence;
- the anticipated impact of the plan on reliability, with an action plan to address any increased risk while the plan is being carried out;
- a timetable with a completion date; and
- implementation milestones, typically no more than three months apart.

The plan is signed by an officer, employee, attorney or other authorized representative. Additional violations can be found for not completing work tied to accepted milestones.

Read the list again. Three of the items are about cause and recurrence.

8.3 When the Plan Is Due

An entity that does not contest the Alleged Violation and penalty must submit its plan within 30 days after being served the notification, or the plan is reflected in the settlement agreement or Notice of Penalty. An entity that contests must submit within ten business days after the Hearing Body's written decision affirming the violation, unless it appeals to NERC. It can also submit while it contests, and that submission is not an admission of the violation or of the penalty.

Waiting has a cost. If no plan has been submitted, or a submitted plan is rejected, later violations of the same standard found before the Hearing Body's decision are not held in abeyance and are treated as repeat violations (Section 6.3).

8.4 Review and Acceptance

The CEA has 60 days to accept or reject a plan, or it is deemed accepted, unless the CEA extends the review by notice. A rejection comes with written reasons. The CEA has 30 days to act on a revision, and a second rejection lets the entity request a hearing.

The Regional Entity sends an accepted plan to NERC within five business days, and NERC has 60 days to approve or disapprove it. NERC submits approved plans to FERC as non-public information within seven business days.

8.5 Implementation, Extensions and Abeyance

The plan is carried out on its terms. The CEA can extend the deadline for good cause, such as an outage that cannot be scheduled or construction that takes longer than planned. Extension requests must reach the CEA before the original date. The CEA can accept a late request for good cause.

Abeyance is the incentive. If the plan runs past the next reporting or assessment period, sanctions for violations of the same standard during implementation are held in abeyance and waived when the plan is satisfactorily completed. The reverse also holds. If the required actions are not completed by the deadline, including extensions, violations during the original period are enforced immediately, a new plan is required, and the CEA can audit the entity or issue a Remedial Action Directive (Section 6.6).

8.6 Completion and Verification

When the plan is done, the entity certifies to the CEA that every required action is complete and keeps documents, data and information sufficient for the CEA to verify it. The CEA can follow up with requests, assessments, spot checks or audits.

The ERO Enterprise tracks how fast mitigation happens. NERC's 2025 annual report states that about 73 percent of noncompliance filed in the past five years had completed mitigation before, or within six months of, being reported to a Regional Entity.

End-of-Chapter Summary

Every noncompliance must be mitigated, and a Mitigation Plan is not an admission. The plan must fix the instance, the cause and recurrence. Completed plans earn waiver of sanctions held in abeyance; missed deadlines bring immediate enforcement.

> **From the Field**
>
> Mitigation that addresses symptom and ignores cause buys you the same finding next cycle. Causation is the audit-defensible response.

9 Penalties, Sanctions, and Regulatory Review

9.1 The Statutory Frame

Two rules sit above everything in the Sanction Guidelines. Under FPA Section 215(e)(6) and 18 C.F.R. § 39.7(g), any penalty must bear a reasonable relation to the seriousness of the violation and take into consideration the entity's efforts to remedy it in a timely manner. And a penalty can be monetary or non-monetary, including a limitation on an activity, function or operation, or placement on a reliability watch list of major violators.

The Sanction Guidelines (Appendix 4B) are the penalty guidelines FERC requires under § 39.7(g)(2). NERC and the Regional Entities follow them while retaining discretion to deviate from the recommended ranges for each factor, using professional judgment to reach a penalty that bears a reasonable relationship to the seriousness of the violation.

9.2 When a Penalty Is Warranted at All

Section 2.1 of the Sanction Guidelines starts with the threshold question. Multiple serious-risk violations or systemic or programmatic failures should typically result in monetary or non-monetary penalties. One or a few minimal, moderate or serious-risk violations may or may not, depending on how the violation was identified, how long it lasted, and the entity's compliance history. NERC and the Regional Entities can impose a zero-dollar penalty where appropriate. Noncompliance processed as a Compliance Exception or FFT carries no penalty at all. Monetary penalties are not available against federal entities, as the Sanction Guidelines note, citing *Southwestern Power Administration v. FERC*, 763 F.3d 27 (D.C. Cir. 2014).

9.3 The Ceiling

In the United States, the maximum monetary penalty for a violation of a requirement equals the current inflation-adjusted maximum civil penalty in 18 C.F.R. § 385.1602(d). As of October 2026, that figure is $1,584,648 per violation, per day, last adjusted in January 2025. The VRF and VSL table in the Sanction Guidelines still shows $1,291,894 in its top cell because the guidelines took effect in January 2021 and cite the 2020 figure; the regulation controls.

Days and instances add up. The guidelines allow a separate penalty for each day a violation continues and for multiple violations of the same requirement on the same day. For a discrete event monitored only periodically, the violation is deemed to start on the first day of noncompliance and continue until it is fixed, regardless of when monitoring found it.

9.4 How the Number Is Built

Section 3 sets a three-step calculation.

Step 1: Base penalty. Start with the VRF and VSL table, which gives a per-day range for each combination. The Lower VRF, Lower VSL cell runs from $1,000 to $3,000 per day. The top cell, High VRF and Severe VSL, starts at $20,000. The guidelines generally start at the low end of the range and adjust for entity size (generating capacity, line miles or peak load), assessed risk, violation duration and Violation Time Horizon.

Step 2: Aggravating and mitigating factors. The guidelines list these:

Aggravating	Mitigating
Repetitive violations and compliance history	Presence and quality of an internal compliance program
Failure to comply with a Remedial Action Directive	Degree and quality of cooperation
Intentional violation (presumption: double the penalty; an economic choice to violate counts as intentional)	Self-reporting and voluntary Mitigating Activities
Concealment (presumption: double), or resistance, non-responsiveness and lack of cooperation	
Management involvement or willful ignorance (presumption: double)	

Step 3: Final adjustments. Credit for settling in good faith without undue delay, and further credit where the entity clearly accepts responsibility. Disgorgement of any profits from an economic choice to violate. Significant reduction or elimination for unique extenuating circumstances such as a significant natural disaster or pandemic. And, on written request with verifiable financial information, review of the entity's ability to pay.

The guidelines also say an entity cannot be penalized more solely because it has no internal compliance program or a poor one. A footnote adds that the lack of controls can still raise the assessed risk or indicate that management was willfully ignorant of the potential for a violation.

9.5 A Penalty Must Not Be a Cost of Doing Business

Section 2.4 of the Sanction Guidelines aims for penalties that are consequential enough that entities do not treat them as an economic choice or a cost of doing business. In the most significant cases, NERC or the Regional Entity can review the entity's public financial information and increase the penalty, up to the maximum, and must explain that analysis in the Notice of Penalty. Penalties are assessed against the entity, not against each registered function, and multiple violations can be penalized individually or with one aggregate penalty.

9.6 Non-Monetary Sanctions

Non-monetary penalties are not the same as mitigation. Section 4 of the Sanction Guidelines says they are not actions an entity would need to take to mitigate or return to compliance. The listed examples include requiring the CEO or equivalent to sign the settlement agreement, periodic reporting to the entity's board or to the NERC Board of Trustees Compliance Committee, a public or non-public letter of reprimand, additional or more frequent compliance

monitoring, and placement on a reliability watch list. They can be imposed instead of, or in addition to, a monetary penalty.

9.7 Review by NERC and FERC

Penalties are reviewed twice. NERC reviews Regional Entity penalties and settlements for consistency before it files. FERC then has the Notice of Penalty. Under 18 C.F.R. § 39.7(e), the entity or FERC on its own motion can seek review within 30 days of filing. If no one does, the penalty is affirmed by operation of law when the 30 days run. An application for review does not stay the penalty unless FERC orders it. FERC acts on an application within 60 days unless it sets a different procedure, and it can affirm, set aside, modify or remand.

9.8 What the Numbers Show

Most noncompliance never reaches a penalty. NERC's 2025 annual report states that the ERO Enterprise processed about 83 percent of filed or submitted noncompliance as Compliance Exceptions and about 14 percent as FFTs, neither of which involves a settlement agreement or a monetary penalty. The rest went through Spreadsheet Notices of Penalty and Full Notices of Penalty, which address more significant noncompliance and involve settlements and, in many cases, monetary or non-monetary sanctions.

End-of-Chapter Summary

Penalties must bear a reasonable relation to seriousness and credit timely remediation. The ceiling is $1,584,648 per violation, per day as of October 2026. The Sanction Guidelines build the number from a VRF and VSL base, adjust it for behavior, and make final adjustments for settlement, disgorgement, extenuating circumstances and ability to pay. Non-monetary sanctions stand apart from mitigation. NERC reviews for consistency, and every filed penalty is subject to FERC review.

> **From the Field**
>
> Penalties scale to risk and to behavior, not to paperwork. The same finding produces different penalties depending on what you did before, during, and after.

10 Due Process, Transparency, and Appeals

10.1 Notice and an Opportunity for Hearing

Due process in CMEP starts with the statute. Section 215(e)(1) of the Federal Power Act allows the ERO to impose a penalty only after notice and an opportunity for a hearing. Appendix 4C builds that into each step: the Notice of Preliminary Screen, the NAVAPS with its 30-day election, the response and conference, the right to request a hearing, and the right to submit a written explanatory statement that accompanies the FERC filing and the public posting.

10.2 The Hearing

An entity that contests an Alleged Violation or penalty can choose a short-form procedure or the general hearing procedure in Attachment 2 to Appendix 4C. The hearing runs before a Hearing Body under Attachment 2 or the hearing procedure in effect for the CEA. Attachment 2 also provides an expedited procedure for contested Remedial Action Directives and a hearing route for a twice-rejected Mitigation Plan.

10.3 Appeals to NERC

Under Rules of Procedure Section 409, the entity or the Regional Entity acting as CEA can appeal a final Hearing Body decision on an Alleged Violation, a proposed penalty, a proposed Mitigation Plan or a proposed Remedial Action Directive. The rules:

- The notice of appeal goes to NERC's Director of Enforcement no later than 21 days after the final decision.
- It must include the full decision, a concise statement of the errors, the relief sought, and supporting argument. No new factual material is allowed that was not presented to the Hearing Body.
- The Clerk files the record within 21 days. Other participants respond within 35 days of the notice, and the appellant may reply within 7 days.
- The Board of Trustees Compliance Committee decides within 180 days, unless it extends for good cause.

On appeal, NERC affirms or remands. After NERC's decision, the penalty still goes to FERC, and the entity can seek FERC review under § 39.7(e).

10.4 What Stays Confidential, and Until When

Confidentiality is the default during enforcement. Under 18 C.F.R. § 39.7(b)(4), each violation or alleged violation is treated as non-public until it is filed with FERC as a Notice of Penalty or resolved by an admission, a settlement or another negotiated disposition. The disposition of a violation that relates to a Cybersecurity Incident, or that would jeopardize Bulk-Power System

security if disclosed, stays non-public unless FERC directs otherwise. Compliance Investigations are confidential unless FERC directs otherwise. Settlements are confidential until NERC approves them.

CIP matters get extra protection. NERC's 2025 annual report states that NERC requests that CIP noncompliance filings to FERC be treated as Critical Energy Infrastructure Information in their entirety, and that it does not publicly post CIP audit reports or CIP noncompliance filings and submittals.

10.5 What Becomes Public

Transparency follows resolution. Under Rules of Procedure Section 401.11, once an entity agrees with a resolution, settles, or exhausts or forgoes its appeals, NERC publicly posts information on each noncompliance, penalty, settlement, and final audit or investigation report, subject to the governmental authority's rules and the confidentiality rules. Each posting includes the entity's name, the nature, time period and circumstances of the noncompliance, the Mitigation Plan or Mitigating Activities, and enough facts for other entities to judge whether they are doing the same thing. Critical infrastructure information and Confidential Information are redacted. The entity may provide its own statement, on letterhead and signed.

That last element is the industry's lesson-learned channel. Read the posted Notices of Penalty for your functions. Somebody else already paid for that education.

10.6 Fairness in the Team Itself

Due process also covers who does the reviewing. Audit team members must be free of conflicts under the CEA's policies; employees or contractors of the audited entity cannot serve as auditors. Team members must sign confidentiality agreements or acknowledgments and complete required NERC or NERC-approved auditor training. The entity has the objection rights described in Chapters 5 and 7. Observers and attendees do not participate in conducting the audit or making findings.

End-of-Chapter Summary

Due process means notice and an opportunity for hearing before any penalty, a choice of hearing procedures, a 21-day appeal to NERC with a 180-day decision target, and FERC review of any filed penalty. Violations stay non-public until a Notice of Penalty or negotiated resolution, and CIP matters stay protected. Resolved matters are posted with enough facts for others to learn from them.

11 Common Misconceptions About Compliance and Enforcement

11.1 "Compliance Means Reliability"

It doesn't. Compliance means the evidence showed the requirements were met. Reliability is how the system performs under real conditions. A system can be compliant and still have problems, and a noncompliance does not necessarily affect the delivery of power. The standards set a minimum level of performance at a point in time. They are not a guarantee against every risk. That is my view from both sides of the audit table, and it is the reason this series exists.

11.2 "Enforcement Is About Punishment"

The data say otherwise. As Section 9.8 shows, most noncompliance in 2025 closed as Compliance Exceptions or FFTs, with no settlement agreement and no monetary penalty. Penalties are real, they can be large, and they are meant to be consequential. But the program's center of gravity is finding, fixing and preventing recurrence.

11.3 "Guidance Is Binding"

It isn't. The Standard Processes Manual, Appendix 3A to the Rules of Procedure, states that the only mandatory and enforceable components of a Reliability Standard are its applicability, its Requirements and its effective dates. The other components are there for information and to show how compliance will be assessed.

Compliance Guidance comes in two types under the ERO Enterprise's Compliance Guidance Policy. Implementation Guidance gives industry-vetted, ERO-endorsed examples of how an entity could comply. CMEP Practice Guides address how ERO Enterprise CMEP staff carry out monitoring and enforcement. Both are useful. Neither adds a requirement. Treat them as evidence of how the auditor will think, not as the rule.

11.4 "Self-Reporting Just Invites Enforcement"

Section 6.2 covers the credit self-reporting earns and when it ends. An entity that sits on a known problem until the audit trades a mitigating factor for a finding.

11.5 "Intent Is What Matters"

The violation question turns on whether the requirement was met. Intent enters at the penalty stage, and it works against the entity. Under the Sanction Guidelines, an intentional violation carries a presumption of doubling the penalty, and a violation attributable to an economic choice is treated as intentional. Concealment and management involvement each carry the same presumption.

11.6 "An Audit Is a Performance Review"

It isn't. Audits cover the standards in scope for a defined audit period. They do not measure the operational effectiveness of an organization's engineering practices or the competence of its people beyond the scope of the audited requirements. The draft audit report may note areas of concern and recommendations, but the findings answer one question about the evidence.

11.7 "A Self-Certification Clears Us"

Receipt of a Self-Certification or a Periodic Data Submittal is not a finding of compliance. Appendix 4C says so in both sections. The CEA can test either one with a spot check.

11.8 "Paying the Penalty Settles the Obligation"

It doesn't. Appendix 4C states that imposing and accepting penalties is not an acceptable alternative to the continuing obligation to comply. A penalty closes the enforcement action. It does not close the requirement.

End-of-Chapter Summary

Compliance is not reliability. Enforcement mostly resolves minimal and moderate risk without penalties. Only applicability, Requirements and effective dates are enforceable; guidance is not. Self-reporting earns credit. Intent aggravates penalties rather than excusing violations. Audits and Self-Certifications are not verdicts on the whole program, and a penalty never replaces compliance.

12 Compliance Oversight in Practice and Ongoing Evolution

12.1 An Annual Cycle

Oversight runs on a yearly rhythm. NERC sets risk elements and posts the ERO CMEP Implementation Plan on or about November 1 for the next year. Regional Entities apply those priorities through each entity's IRA and Compliance Oversight Plan. Audits, spot checks and Self-Certifications follow. Findings, event analysis and data feed next year's risk elements, and NERC staff periodically review noncompliance reports to identify trends (ROP Section 401.12).

12.2 Faster Processing of Minimal Risk

NERC's 2025 annual report describes a multi-year effort, prompted by FERC's orders on the 2024 Five-Year Performance Assessment, to process minimal-risk Compliance Exceptions within 180 days on average. The goals are faster feedback on the standards, more attention on higher risk, and less tracking burden for industry. The report also shows 17 percent more dispositions filed and submitted in 2025 than in 2024.

12.3 Oversight Is Becoming a Data Exchange

More of CMEP now runs through ERO systems. The ERO Enterprise's Align system handles enforcement, mitigation, IRAs, Compliance Oversight Plans, audits and spot checks, Periodic Data Submittals and Self-Certifications; NERC reported six Align releases in the first half of 2025. For CIP evidence, the ERO Enterprise publishes a CIP Evidence Request Tool and user guide.

In my view, the practical consequence is that evidence quality is now visible earlier. An entity whose evidence is clean, dated and traceable at the source answers a data request in days. An entity that rebuilds evidence for every engagement answers in weeks, and it shows.

12.4 New Entities, Same Program

NERC's inverter-based resource registration initiative brought Category 2 Generator Owners and Generator Operators onto the NERC Compliance Registry with an effective registration date of May 15, 2026. On October 1, 2026, PRC-029-2, the ride-through standard for inverter-based resources, took effect following FERC approval, replacing PRC-029-1. The procedures in Appendix 4C will keep changing. The test underneath them will not: can the entity show, with evidence, that it did what the standard requires, and did it work?

End-of-Chapter Summary

CMEP runs on an annual risk cycle and keeps evolving. The evidentiary test does not.

Glossary

Term	Meaning in this paper
Alleged Violation	A potential noncompliance for which the Compliance Enforcement Authority has determined, based on an assessment of the facts and circumstances, that evidence exists to indicate a registered entity has violated a Reliability Standard, and that will be resolved outside the Compliance Exception or FFT processes. (ROP Appendix 2)
Bulk Electric System (BES)	As defined in the NERC Glossary of Terms: unless modified by the definition's listed inclusions and exclusions, all Transmission Elements operated at 100 kV or higher and Real Power and Reactive Power resources connected at 100 kV or higher. It does not include facilities used in the local distribution of electric energy.
Compliance Audit	A systematic, objective review and examination of records and activities to determine whether a registered entity meets the requirements of applicable Reliability Standards. (ROP Appendix 2)
Compliance Enforcement Authority (CEA)	NERC or the Regional Entity, in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards. (ROP Appendix 2)
Compliance Exception	A noncompliance addressed under Appendix 4C that is not pursued through an enforcement action under Section 5.0; used for minimal-risk noncompliance. (ROP Appendix 2; Appendix 4C, Section 4A.1)
Compliance Investigation	A comprehensive investigation, which may include an on-site visit with interviews of the appropriate personnel, to determine whether a violation of a Reliability Standard has occurred. (ROP Appendix 2)
Compliance Monitoring and Enforcement Program (CMEP)	The program NERC and the Regional Entities use to monitor, assess and enforce compliance with Reliability Standards, set out in Appendix 4C to the NERC Rules of Procedure.
Confirmed Violation	An Alleged Violation that the entity has accepted or not contested, that a final order of NERC or a Hearing Body has found, for which the period to request a hearing or appeal has expired, or that the entity has settled. (ROP Appendix 2)
Find, Fix, Track and Report (FFT)	A streamlined process to resolve minimal or moderate risk, remediated noncompliance that is not assessed a financial penalty. (ROP Appendix 2)
Inherent Risk Assessment (IRA)	The CEA's review of the potential risks an individual registered entity poses to the reliability of the Bulk Power System, considering factors such as assets, system, geography, interconnectivity and prior compliance history. (ROP Appendix 2)

Term	Meaning in this paper
Mitigating Activities	Actions taken by a registered entity to correct and prevent recurrence of a noncompliance, whether or not they are embodied in a Mitigation Plan. (ROP Appendix 2)
Mitigation Plan	An action plan developed by the registered entity to correct a noncompliance with a Reliability Standard and prevent re-occurrence of the violation. (ROP Appendix 2)
Notice of Penalty	A notice prepared by NERC and filed with FERC, following NERC's approval of a Confirmed Violation or a settlement agreement, stating the penalty or sanction imposed or agreed to. (ROP Appendix 2)
Preliminary Screen	The CEA's initial evaluation of evidence of potential noncompliance: whether the entity is registered, whether the requirement applies to a function for which it is registered, and whether the matter duplicates one already in process. (ROP Appendix 2)
Remedial Action Directive	An action, other than a penalty or sanction, required by a CEA to bring an entity into compliance or avoid a violation, that is immediately necessary to protect the Bulk Power System from an imminent or actual threat. (ROP Appendix 2)
Self-Certification	An attestation by a registered entity that it is compliant or noncompliant with the requirement, that it does not own Facilities subject to it, or that the requirement does not apply to it. (ROP Appendix 2)
Self-Logging	A process by which entities found eligible by a CEA after a formal review of internal controls record potential noncompliance on a log instead of submitting individual Self-Reports. (ROP Appendix 2)
Self-Report	A report by a registered entity stating that it believes it has, or may have, violated a Reliability Standard. (ROP Appendix 2)
Spot Check	A process in which the CEA requests information to support a Self-Certification, Self-Report or Periodic Data Submittal and assess compliance, as a random check, or in response to operating problems or system events. (ROP Appendix 2)
Violation Risk Factor (VRF)	The Lower, Medium or High rating assigned to each requirement through the standards development process to indicate the expected or potential impact of a violation on the reliability of the Bulk Power System. (Sanction Guidelines, Appendix 4B)
Violation Severity Level (VSL)	The Lower, Moderate, High or Severe level assessed after a violation to indicate the degree to which the requirement was violated. (Sanction Guidelines, Appendix 4B)

This glossary is intended to convey a general understanding of terms as they are used in this reference. It does not change or supersede the definitions in the NERC Glossary of Terms or Appendix 2 to the NERC Rules of Procedure.

How Energy Compliance Can Help

CMEP rewards the entity that finds its own problems, fixes the cause, and can prove both. Here is where we help.

Audit preparation and audit defense

EC provides NERC compliance program support, interpretation and audit preparation; audit and enforcement support (non-advocacy); and audit defense, including Notice of Penalty response and settlement posture. EC also handles RSAW production and data request strategy.

Self-Reports, mitigation and program reviews

EC provides mitigation planning and Self-Report development. Regulator-perspective program reviews and reliability governance and program assessments test the program; compliance program design and improvement strengthens it.

Advisory, registration and engagement

EC also provides NERC reliability and compliance advisory support, senior advisory with direct engagement on complex reliability questions, registration and applicability analysis, operational and engineering reliability alignment, training and executive briefings on reliability frameworks, and industry engagement in standards development and working-group participation. Each engagement is scoped to the entity's role, function and bulk system impact, and every engagement is overseen by a senior practitioner.

WattOps Compliance

Every CMEP process runs on evidence. WattOps Compliance is EC's NERC compliance evidence platform (wattopscompliance.com). EC will run one standard at one facility through WattOps at no cost (CIP standards excluded).

RenewOps

For renewable and storage operators, operations data carries the compliance position. RenewOps is EC's renewable operations monitoring and analytics platform, with a Data Center module.

Audit notice or NAVAPS on your desk? Call before you answer it.

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

- Federal Power Act Section 215, Electric Reliability, 16 U.S.C. § 824o, as added by the Energy Policy Act of 2005, Pub. L. 109-58, § 1211 (including statutory note on the status of the ERO). https://www.law.cornell.edu/uscode/text/16/824o
- 18 C.F.R. § 39.7, Enforcement of Reliability Standards (eCFR, current as of Oct. 22, 2026). https://www.ecfr.gov/current/title-18/chapter-I/subchapter-B/part-39/section-39.7
- 18 C.F.R. § 385.1602, Civil penalties, as adjusted (eCFR, current as of Oct. 23, 2026; last amended Jan. 14, 2025). https://www.ecfr.gov/current/title-18/section-385.1602
- FERC, Mandatory Reliability Standards for the Bulk-Power System, Order No. 693, Docket No. RM06-16-000, 72 Fed. Reg. 16416 (Apr. 4, 2007). https://www.govinfo.gov/content/pkg/FR-2007-04-04/pdf/E7-5284.pdf
- FERC, Order on the Electric Reliability Organization's Five-Year Performance Assessment, 149 FERC ¶ 61,141, Docket No. RR14-5-000 (Nov. 20, 2014) (citing the ERO Certification Order, 116 FERC ¶ 61,062 (2006)). https://www.ferc.gov/sites/default/files/2020-05/E-10_9.pdf
- NERC, Rules of Procedure (effective Nov. 28, 2023), Sections 400 (including 401, 402, 409), 800 (including 807) and 1500. https://www.nerc.com/globalassets/who-we-are/rules-of-procedure/nerc-rop.pdf
- NERC, Definitions Used in the Rules of Procedure, Appendix 2 to the Rules of Procedure (effective June 27, 2024). https://www.nerc.com/globalassets/who-we-are/rules-of-procedure/appendix-2.pdf
- NERC, Standard Processes Manual, Appendix 3A to the Rules of Procedure (effective Nov. 28, 2023). https://www.nerc.com/globalassets/who-we-are/rules-of-procedure/appendix-3a.pdf
- NERC, Sanction Guidelines of the North American Electric Reliability Corporation, Appendix 4B to the Rules of Procedure (effective Jan. 19, 2021). https://www.nerc.com/globalassets/who-we-are/rules-of-procedure/appendix-4b.pdf
- NERC, Compliance Monitoring and Enforcement Program, Appendix 4C to the Rules of Procedure (effective May 19, 2022), including Attachment 1 and Attachment 2, Hearing Procedures. https://www.nerc.com/globalassets/who-we-are/rules-of-procedure/appendix-4c.pdf
- NERC, ORCP and CMEP Annual Report (Feb. 11, 2026) (2025 data). https://www.nerc.com/globalassets/programs/enforcement/cmep-and-vegetation-reports/2025-orcp-and-cmep-annual-report.pdf
- ERO Enterprise, CMEP Practice Guide: Evaluation of Facility Ratings and System Operating Limits (June 17, 2020) (description of the Compliance Guidance Policy,

Implementation Guidance and CMEP Practice Guides). https://www.nerc.com/pa/comp/guidance/CMEPPracticeGuidesDL/ERO%20Enterprise%20CMEP%20Practice%20Guide_%20Evaluation%20of%20Facility%20Ratings%20and%20System%20Operating%20Limits.pdf

- ERO Enterprise, CIP Evidence Request Tool User Guide (January 2026), NERC CMEP Resources. https://www.nerc.com/globalassets/programs/compliance/cmep-resources/cip-evidence-request-tool-user-guide-v10.pdf
- NERC, Glossary of Terms Used in NERC Reliability Standards (definition of Bulk Electric System). https://www.nerc.com/glossary-of-terms
- NERC, PRC-029-2, Frequency and Voltage Ride-through Requirements for Inverter-Based Resources. https://www.nerc.com/globalassets/standards/reliability-standards/prc/prc-029-2.pdf
- WECC, FAQ: Inverter-Based Resource Registration Initiative, Category 2 GO and GOP Registration Process (2026). https://www.wecc.org/sites/default/files/documents/program/2026/faq-ibr-registration-initiative-category-2-go-and-gop-registration-process.pdf

© Energy Compliance, Inc. · EC-WP-104 · October 2026