SPECIAL TOPICS SERIES · EC-WP-603

Self-Reporting Strategy

When to file, what to disclose, how to scope, and the long-term program effect.

In my view, Self-Reporting is the most under-managed strategic decision in NERC compliance. This reference walks through what the CMEP and the Sanction Guidelines actually say about Self-Reports, then covers the decisions a program has to get right on timing, scope and mitigation. The aim is a Self-Report record that strengthens the program's standing with its Regional Entity year after year.

energycomplianceinc.com

OCTOBER 2026

Disclaimer & Legal Notice

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

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

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

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

Foreword

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

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

The entities that do reliability well share a common habit. They take the standards seriously without confusing them with reliability itself. A NERC Reliability Standard is a floor, not a ceiling. An auditor evaluates compliance; a system either delivers reliability or it doesn't. These entities 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, whether a standard family, an operational function, a regulatory framework, or an emerging industry challenge, and walks through how it actually works.

They're 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, grounded in evidence, and 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, and 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 and apply it well. And remember the only test that ultimately matters: when the system needs to perform, does it?

Rob Smith

Founder and Principal, Energy Compliance, Inc.

Executive Summary

In my view, Self-Reporting is the most under-managed strategic decision in NERC compliance. The rules reward it. The NERC Sanction Guidelines treat a prompt Self-Report, filed before a compliance monitoring engagement finds the issue, as a mitigating factor that can reduce the base monetary penalty by up to 30 percent. The ERO Enterprise reads high levels of self-reported noncompliance as a sign of good detective controls and a strong culture of compliance. Registered entities already self-identify about 85 percent of reported noncompliance, and about 97 percent of the noncompliance processed in 2025 was resolved as Compliance Exceptions or Find, Fix, Track and Report items, which carry no monetary penalty.

Yet many programs still treat Self-Reporting as something to avoid: an admission of failure, an invitation to scrutiny. That framing misreads the regulator. In my experience the regulator reads a well-built Self-Report as evidence of program maturity, and programs that internalize this build enforcement records that improve over years.

The key points:

- A Self-Report is not an admission of failure. Done well, it is evidence that the program's detective controls work, and the ERO Enterprise says it reads it that way.
- The credit is real but conditional. It depends on reporting within a reasonably prompt time and before detection through an audit, spot check or Self-Certification.
- Timing matters. The Sanction Guidelines say to file as soon as practical, typically within three months of discovery, and to add information as it becomes known. A notification letter for an upcoming engagement generally ends Self-Report credit for the requirements in its scope.
- Scope matters. Under-disclosure produces a worse outcome than full disclosure. Cooperation credit should include disclosure of all pertinent information, and concealment carries a presumption that the penalty doubles.
- The mitigation that travels with the Self-Report shapes the resolution. The CMEP expects every Self-Report to describe the extent, the cause and the mitigation.
- In my view, a program that hasn't Self-Reported in five years is either exemplary or invisible, and the Region will want to know which.
- Self-Reports compound. The Region's view of the program is shaped by the record over years, not by single events.

1 What the Rules Actually Say

Before strategy, the mechanics. The rules that govern Self-Reports are short, public and specific. Most of the bad Self-Report decisions I've seen started with someone who had never read them.

1.1 What a Self-Report Is

The NERC Rules of Procedure define a Self-Report as a report by a registered entity stating that it believes it has, or may have, violated a Reliability Standard. Note the "may have." The threshold for filing is not certainty.

Section 4.5 of the Compliance Monitoring and Enforcement Program (CMEP), Appendix 4C to the Rules of Procedure, encourages Self-Reports at the time an entity becomes aware that it has, or may have, violated a standard. It also says what goes in one: 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 Compliance Enforcement Authority (the Regional Entity, in most cases) reviews the Self-Report and may ask for clarification or additional documents, data and information.

1.2 The Self-Report Credit in the Sanction Guidelines

The NERC Sanction Guidelines, Appendix 4B to the Rules of Procedure, list disclosure through Self-Reporting and voluntary Mitigating Activities as 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 whether it did so before detection through a compliance monitoring engagement (a Compliance Audit, Spot Check or Self-Certification).

The Guidelines put numbers on the adjustment ranges. The ones that matter most for Self-Reporting are these:

Factor	Effect on the Base Monetary Penalty
Self-Report (mitigating)	Reduction of 0% to 30%
Internal compliance program (mitigating)	Reduction of 0% to 40%
Cooperation (mitigating)	Reduction of 0% to 20%
Repeat violations (aggravating)	Increase of 0% to 800%
Concealment or impediment (aggravating)	Increase of 0% to 800%

Two of those mitigating factors are tied to how a program Self-Reports. Cooperation credit requires cooperation that is both timely and thorough, starting at essentially the same time the

entity reports or becomes aware of the violation, and including disclosure of all pertinent information the entity knows. The internal compliance program factor looks at due diligence to prevent and detect violations and at the culture of compliance. A program that finds and reports its own problems is showing both.

1.3 The Three-Month Expectation and the Notification Cutoff

The Sanction Guidelines answer the timing question directly. An entity should submit a Self-Report as soon as practical, typically within three months of discovery, and provide additional or more comprehensive information as it becomes known. NERC and the Regional Entity keep discretion to give credit outside that period based on the facts.

The second timing rule is the one that catches programs. Receipt of a notification letter for an upcoming compliance monitoring engagement, listing the standards and requirements in scope, generally ends eligibility for Self-Report credit on those requirements until the engagement is over. A known issue sitting in the internal queue when the audit notice arrives has lost most of its value as a Self-Report.

1.4 Where Self-Reports End Up

Most noncompliance does not end in a penalty. The CMEP provides streamlined alternatives to a full enforcement action: the Compliance Exception process for minimal risk noncompliance, and Find, Fix, Track and Report (FFT) for minimal or moderate risk noncompliance. Compliance Exceptions are not included in an entity's compliance history for penalty purposes, with one caveat. The Regional Entity must consider a history of Compliance Exceptions where a failure to fully remediate contributes to a later serious or substantial noncompliance.

NERC's 2025 ORCP and CMEP Annual Report, published February 11, 2026, shows how this plays out. In 2025 roughly 85 percent of reported noncompliance was self-identified by registered entities, the same share as the five-year average. About 83 percent of noncompliance filed or submitted in 2025 was processed as Compliance Exceptions and 14 percent as FFTs. The report states that the ERO Enterprise looks for high levels of self-reported noncompliance as an indicator of good detective controls and strong cultures of compliance.

Entities that pass a formal review of their internal controls can be approved for Self-Logging. They record minimal risk noncompliance on a log instead of filing individual Self-Reports, with a rebuttable presumption that logged items are resolved as Compliance Exceptions. The Regional Entity reviews the log at least every three months, with the possibility of extending that to six.

> **From the Field**
>
> The threshold for a Self-Report is "has, or may have." The credit depends on being prompt and being first. Three months from discovery is the typical expectation, and the audit notification letter closes the window on everything in its scope.

2 The Self-Report Decision Framework

Self-Report decisions deserve a defined framework. Filing commits the entity to formal disclosure and shapes its enforcement posture, and ad hoc decisions produce inconsistent outcomes that are their own exposure.

2.1 Classification

A defined framework starts with classification. Is the matter a confirmed violation, a likely violation, or a question that needs further investigation? Confirmed violations call for a Self-Report. Likely violations call for an investigation that, if it confirms the issue, leads to a Self-Report. Questions call for analysis that may or may not lead to either. Remember the CMEP threshold is "has, or may have": a likely violation that is slow to confirm is usually a candidate for an early report and later supplements.

2.2 Timing

From the moment of discovery, how long does internal analysis take before the Self-Report is filed? The Sanction Guidelines set the reference point: as soon as practical, typically within three months. In my view a short, documented analysis window signals a program that works. A gap well past three months without a reason signals a program that delays disclosure.

2.3 Authority

Who decides? The senior compliance leader, general counsel, the program manager? Decision authority shapes how the matter is treated internally and how it is communicated to the Region. Write it into the procedure, with a backup.

2.4 Documentation

Document every Self-Report decision internally: the analysis, the timing, the rationale and the disclosure scope. That record supports the program if the Region later questions the decision, and it supports consistency the next time a similar matter comes up. Undocumented decisions get reconstructed later by people who weren't in the room.

> **From the Field**
>
> Name who decides, measure the gap from discovery to filing against the three-month expectation, and write down why you decided what you decided.

3 What the Region Actually Sees When You Self-Report

3.1 The Self-Report Enters an Existing File

A Self-Report doesn't arrive in a vacuum. The Regional Entity reviews it to evaluate compliance and may come back with questions or requests for more information. Like any potential noncompliance, it goes through a Preliminary Screen, which the CMEP requires within ten business days after the potential noncompliance is identified. The screen is narrow: is this a registered entity, and is the requirement applicable, approved and in effect for the period at issue?

The matter then joins everything else the Region knows about the entity, including its Inherent Risk Assessment, which considers prior compliance history, and its recent audit findings.

3.2 How Context Changes the Reading

Against a clean record, a Self-Report reads as a mature program finding its own issues. Against a run of recent findings, it can read as compounding problems or as a program being candid about a hard stretch. Which reading wins depends on how clear the pattern of disclosure is.

3.3 How the Content Changes the Reading

Content matters as much as context. A complete, well-documented Self-Report signals competence; a vague or partial one raises questions about competence or candor.

Programs that Self-Report well make it easy for the Region to read the matter quickly and accurately. The facts are clear, the extent, cause and mitigation are stated as CMEP Section 4.5 expects, and a knowledgeable contact is named.

> **From the Field**
>
> A Self-Report lands in the Region's existing view of the entity. Under-disclosure usually gets found. Self-Reports that make the Region's job easy resolve faster.

4 Timing: When Speed Matters and When It Doesn't

4.1 Pace, Not Just Speed

Self-Report timing is about the right pace for the matter. Some matters need fast filing because the Region is likely to find them or reliability is at risk. Others need investigation first, because an inaccurate Self-Report creates its own problems.

Section 1.3's two rules, file within about three months and supplement as facts develop, mean you rarely have to choose between speed and accuracy. You can file what you know, say clearly what is still under investigation, and update.

4.2 When to File Fast

Fast filing is the right call when:

- the violation is unambiguous;
- the Region is likely to find it independently soon, including when a compliance monitoring engagement is on the horizon;
- the matter has reliability implications that make continued exposure unacceptable; or
- the entity has confirmed the facts and more analysis won't change the disclosure.

4.3 When More Time Is Justified

More time before filing, or before supplementing, is defensible when:

- the matter is ambiguous and needs confirmation that a violation occurred at all;
- the extent of impact needs investigation to characterize accurately;
- the mitigation needs development so the Self-Report can describe it; or
- the matter is complex enough that a hasty report would contain inaccurate content.

Past the three-month mark, file the known facts and open questions rather than stay silent.

4.4 Calibration and the Timeline Record

In my experience, programs that file everything within days sometimes file inaccurate Self-Reports that need correcting, and programs that take six months for everything get overtaken by the Region's own discovery. Calibrated pace is part of program maturity.

> **From the Field**
>
> Match the pace to the matter, inside the three-month expectation. Hasty Self-Reports get corrected later; slow ones get overtaken by the audit notice. If it took 90 days, be ready to explain the 90 days.

5 Scope: How Much to Disclose

Self-Report scope is consequential. Under-disclosure creates worse outcomes than appropriate full disclosure.

5.1 Why Under-Disclosure Fails

A common mistake is disclosing less than the full extent of the matter. The reasoning is usually defensive: limit exposure, narrow the engagement, avoid drawing attention to related issues. It misreads the regulator's process.

The Region's review of a Self-Report includes context. In my experience, reviewers look at related compliance areas, recent history, equipment scope and organizational structure. If the Self-Report describes a narrower matter than the facts support, the Region usually finds the gap. Once it does, the program's posture shifts from "entity that surfaced its own issue" to "entity that tried to under-disclose and got caught." That risks the concealment presumption.

The rules back this up. The CMEP expects a Self-Report to describe the extent of the noncompliance. Cooperation credit under the Sanction Guidelines should include disclosure of all pertinent information the entity knows. And where NERC or the Regional Entity finds that an entity concealed or tried to conceal a violation, or information needed to investigate it, the presumption is to double the monetary penalty otherwise determined.

5.2 Calibrated Full Disclosure

Appropriate full disclosure means reporting the matter as the program understands it, with the scope its investigation actually supports. That is not over-disclosure, which has its own cost: a report broader than necessary can pull the Region into matters that never needed its attention. It is complete, calibrated disclosure of what was investigated and found.

The line between appropriate disclosure and over- or under-disclosure takes judgment. Programs that get it right have legal counsel and senior compliance leadership engaged in the decision. Programs that get it wrong usually work without that engagement and produce Self-Reports that reflect someone's first instinct rather than considered analysis.

5.3 The Cost Recurs

The cost of under-disclosure is high and it recurs. In my experience, later matters from the same entity get read with more skepticism, and that effect builds over years.

> **From the Field**
>
> Under-disclosure is the most common Self-Report mistake, and the Region usually catches it. The goal is calibrated full disclosure: not more than the facts support, not less. That judgment needs counsel and senior compliance leadership in the room.

6 The Mitigation Plan That Travels with the Report

In my experience, a Self-Report with complete, credible mitigation resolves faster than one without. The mitigation is part of the disclosure.

6.1 What the CMEP Requires

The CMEP already expects every Self-Report to describe the actions taken or planned to mitigate the noncompliance and prevent recurrence. Section 6 sets out what a formal Mitigation Plan must contain. Submitting one is not an admission of a violation.

Mitigation Plan element (CMEP Section 6.2)	What it means in practice
Point of contact	A person responsible for filing, technically knowledgeable and authorized to answer status questions
Noncompliance to be corrected	The standards and requirements the plan addresses
Cause	The root cause, not the symptom
Mitigating Activities	Actions to correct the noncompliance, correct its cause and prevent recurrence
Reliability impact	Anticipated effect on the Bulk Power System and how added risk will be managed during implementation
Timetable	The completion date for the whole plan
Milestones	Interim milestones, typically no more than three months apart unless the Regional Entity agrees otherwise

The plan must be signed by an officer, employee, attorney or other authorized representative. The Regional Entity has 60 days from receipt to accept or reject it unless it extends the review period; if it does neither, the plan is deemed accepted. Missing an accepted milestone can itself become an additional violation, so set milestones you will actually hit.

6.2 What a Credible Plan Adds

Beyond the required elements, two things separate a credible plan from a compliant one. First, verification: how will the program confirm the corrective actions worked? Second, evidence: what records will demonstrate completion when the Region asks?

Each element matters. A root cause analysis that is too shallow signals incomplete understanding. Corrective actions that don't address the root cause signal the same thing.

Timelines that are unrealistic in either direction raise questions about program capability. Verification gaps suggest the matter could recur, and evidence gaps mean completion can't be shown.

6.3 The Conversation It Changes

Programs that develop strong mitigation before or with the Self-Report have a different conversation with the Region than programs that file first and work out mitigation later. The first conversation is "here's the issue and here's the path to resolution." The second is "here's the issue, and we'll get back to you." The Region can work with both. In my experience the first resolves faster and leaves a better posture. NERC's 2025 annual report shows how common prompt mitigation already is: roughly 73 percent of noncompliance filed in the past five years had mitigation completed before, or within six months of, being reported to a Regional Entity.

The mitigation plan also forces honest analysis. A credible plan requires an understanding of root cause, which requires an honest look at what happened, which deepens the program's understanding of its own operation. That benefit holds whether or not a regulator ever reads the plan.

> **From the Field**
>
> The CMEP expects extent, cause and mitigation in the Self-Report itself. A credible plan names the root cause, sets milestones you will hit, and says how you'll prove it worked. Vague mitigation signals incomplete understanding, and the Region responds to the signal.

7 Common Self-Report Mistakes

Self-Reporting mistakes repeat, and most programs that mishandle Self-Reports fall into one of a few categories.

7.1 The Seven Recurring Mistakes

1. **Not filing when filing was the right call.** The program decides an internal fix is enough. The matter surfaces later through an audit, the posture is worse for the silence, and after the notification letter the Self-Report credit is generally gone.
2. **Filing too early without enough analysis.** Inaccurate content has to be corrected, and corrections create friction. The fix is not to wait; it is to separate what you know from what you're still investigating.
3. **Under-disclosure.** It limits short-term exposure and creates long-term damage, as Chapter 5 explains.
4. **Filing without mitigation.** The CMEP expects mitigation in the Self-Report.
5. **Hostile or evasive engagement with the Region's follow-up.** A Self-Report opens a conversation. The program's conduct in that conversation shapes the outcome as much as the filing. The Sanction Guidelines treat resistance, non-responsiveness and lack of cooperation as aggravating factors.
6. **Inconsistent quality across matters.** The Region notices.
7. **Not learning across Self-Reports.** Each Self-Report is a lesson about the program. Programs that don't extract the lessons keep filing the same Self-Report, and repetitive violations with the same root cause are an aggravating factor under the Sanction Guidelines.

7.2 Prevention

Each mistake has a prevention, and most of the preventions are procedural: a decision framework, a timeline record, a disclosure review with counsel, a mitigation template, a single point of contact for Regional follow-up, and a periodic look across past Self-Reports for shared causes. The ERO Enterprise's own Self-Reporting and Mitigation training, presented in condensed form to the Compliance and Certification Committee in October 2025, covered what to include in Self-Reports, how to structure submissions and common pitfalls to avoid.

> **From the Field**
>
> Self-Report mistakes repeat, so prevention can be built into procedure. Filing early is fine; filing inaccurately is not. Look across your past Self-Reports for a shared root cause before the Region does.

8 Building a Culture That Self-Reports Effectively

Self-Reporting depends on culture. Programs where staff fear disclosure don't surface issues for Self-Report.

8.1 Why Culture Decides Whether Issues Surface

The process of Self-Reporting is straightforward; the culture behind it is harder. Where staff fear blame or management's reaction, issues don't get surfaced for Self-Report. They surface anyway, through an audit.

The Sanction Guidelines make culture part of the penalty calculation: the internal compliance program factor looks at whether the entity promotes an organizational culture that encourages a commitment to compliance. The ERO Enterprise ties high self-reporting levels to strong cultures of compliance in its 2025 annual report.

8.2 What That Culture Looks Like

A culture that supports effective Self-Reporting has a few recognizable traits:

- Staff who identify potential violations report them up the chain promptly, confident the report will be received as program improvement, not personal failure.
- Senior management treats disclosed issues as program data, not as performance problems for the people who disclosed them.
- Legal counsel treats potential Self-Reports as strategic decisions, not defensive postures.

8.3 The First Response Sets the Pattern

This culture is built over years and reinforced by how management responds when an issue surfaces. The first time a staff member is criticized for surfacing an issue, the message travels. Future issues stop surfacing. The program loses visibility into its own operation.

The reverse is also true. When the program addresses the substance and supports the staff member, that message travels too. More issues surface, Self-Report quality improves, and management gets a truer picture of the program. In my view, programs that build this culture end up with better long-term enforcement records, and the gap widens with time.

> **From the Field**
>
> How senior management responds to the first surfaced issue decides whether the next one surfaces at all. The culture takes years to build and one bad response to damage.

9 The Long-Term Posture Effect

Self-Report records compound over time. In my view, programs that Self-Report well for years build a record that shapes how the Region scopes their audits and reads their next filing.

9.1 Patterns, Not Events

The Region's view of an entity is formed by patterns over years, not single events, and the Self-Report record is a large part of that pattern.

9.2 Where the Record Shows Up

The record shows up in concrete places:

- **Oversight scope.** The Inherent Risk Assessment considers prior compliance history, and the CMEP has the Regional Entity tailor audit scope using risk-based inputs that include Inherent Risk Assessments and internal controls.
- **Penalty calculation.** The Sanction Guidelines weigh repetitive violations and compliance history as an aggravating factor, generally looking at prior violations still ongoing within five years of the start of the current one. A clean history, on its own, earns no reduction; the credit comes from self-reporting, cooperation and the quality of the internal compliance program.
- **Settlement.** The Guidelines allow a reduction for settlement, considering good-faith efforts to settle without undue delay.
- **Disposition.** Compliance Exceptions stay out of compliance history for penalty purposes unless a failure to fully remediate contributes to a later serious or substantial noncompliance.

9.3 The Compounding Runs Both Ways

Programs that Self-Report well, consistently, earn more of the Region's trust over time. Programs with Self-Report failures, under-disclosures or evasive engagement face more scrutiny over time. In my experience, those patterns outlast leadership changes and audit cycles.

Programs that treat Self-Reporting as a strategic asset build the framework, train the staff and execute consistently. Programs that treat it as defensive overhead accept the long-term cost. In my view, over a decade the leaders who think about this strategically have smoother regulatory interactions, and the ones who don't accumulate friction.

> **From the Field**
>
> The Region remembers patterns, not events. A decade of effective Self-Reporting produces a very different enforcement environment from a decade without it.

Glossary

Term	Meaning in this paper
Compliance Enforcement Authority (CEA)	NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.
Compliance Exception	A noncompliance addressed under Appendix 4C and not pursued through an enforcement action. Used for minimal risk noncompliance and not included in compliance history for penalty purposes.
Find, Fix, Track and Report (FFT)	A streamlined process to resolve minimal or moderate risk, remediated noncompliance that is not assessed a financial penalty.
Inherent Risk Assessment (IRA)	The Compliance Enforcement Authority's review of the potential risks an individual registered entity poses to the reliability of the Bulk Power System, considering assets, system, geography, interconnectivity, prior compliance history and other entity-specific factors.
Mitigating Activities	Actions a registered entity takes to correct a noncompliance and prevent recurrence, whether or not they are set out in a Mitigation Plan.
Mitigation Plan	An action plan developed by the registered entity to correct a noncompliance with a Reliability Standard and prevent its recurrence. Its contents are set by CMEP Section 6.2.
Notice of Penalty	A notice prepared by NERC and filed with FERC stating the penalty or sanction imposed or agreed to for a Confirmed Violation or as part of a settlement.
Preliminary Screen	The Compliance Enforcement Authority's initial evaluation of evidence of potential noncompliance, conducted within ten business days after the potential noncompliance is identified.
Sanction Guidelines	The NERC Sanction Guidelines, Appendix 4B to the NERC Rules of Procedure, which set out how penalties are determined, including aggravating and mitigating factors.
Self-Logging	A process by which registered entities found eligible after a formal review of internal controls record minimal risk potential noncompliance on a log instead of filing individual Self-Reports.
Self-Report	A report by a registered entity stating that it believes it has, or may have, violated a Reliability Standard.

How Energy Compliance Can Help

Every chapter in this reference comes back to the same point: a Self-Report is a decision, and the quality of that decision shows up in the record for years. Energy Compliance works on those decisions with registered entities directly.

Mitigation planning and Self-Report development. We help programs decide whether and when to file, scope the disclosure to what the investigation supports, and build the extent, cause and mitigation content the CMEP expects, including Mitigation Plans with milestones the program can meet.

Audit and enforcement support (non-advocacy). When a Self-Report draws Regional follow-up, or an issue surfaces through an audit instead, we help the program respond clearly and completely. That includes Notice of Penalty response and settlement posture.

Compliance program design and improvement. The decision framework, the timeline record, the disclosure review and the culture that surfaces issues are all program design. We build them into procedure, and we review programs from the regulator's perspective so the gaps get found internally first.

WattOps Compliance. WattOps is EC's NERC compliance evidence platform, at wattopscompliance.com. A Self-Report is only as strong as the evidence behind its extent, cause and mitigation, and WattOps is where that evidence lives. We'll run one standard at one facility through WattOps at no cost (CIP standards excluded).

RenewOps. RenewOps is EC's renewable operations monitoring and analytics platform, with a Data Center module. For renewable and storage operators, many potential noncompliance issues first show up in operations data, and RenewOps gives the program that view of its own operation.

If you have a matter sitting in the internal queue, or you haven't Self-Reported in years and aren't sure why, call me. We'll look at it together and decide what it needs.

Website: energycomplianceinc.com · Email: rsmith@complianceforenergy.com

Phone: 763.438.4427

About the Author

Rob Smith is the Founder and Principal of Energy Compliance, Inc., with more than thirty years in the industry on every side of the system. He began in control-room operations as a Reliability Coordinator, Transmission Operator, and Power System Operator across RTO/ISO and utility control centers. On the regulator side, he was a senior compliance auditor and subject matter expert for NERC Reliability Standards. He audited grid facilities, evaluated mitigation adequacy, participated in risk-based oversight of utility mitigation activities, and supported the development of violation notifications and settlements in FERC-directed enforcement actions. He conducted a regulatory audit in the Sultanate of Oman against the Sultanate's Sector Law and Grid Code.

He founded Energy Compliance, Inc. to deliver senior regulator-side compliance authority without the layered staffing and billable-hour overhead of larger firms.

Education:

- MBA, Energy Management, University of Mary
- MSL, Compliance Law, Fordham Law University
- BAS, Energy Management, Bismarck State College
- BAS, Mechanical Engineering, Metallurgy minor, University of Florida
- BAS, Criminology, St. Petersburg College (State Law Enforcement Certification)
- AAS, Power Plant Technology, Bismarck State College
- AAS, Electrical Transmission System Technology, Bismarck State College

Certifications: NERC Lead Auditor training; previously NERC-certified at the Reliability Coordinator level; 1st Class A Boiler Engineer License, Minnesota.

About Energy Compliance, Inc.

Energy Compliance, Inc. is an independent consulting and advisory firm based in Bloomington, Minnesota, focused exclusively on electric reliability, cybersecurity reliability, and regulatory compliance for organizations connected to the North American Bulk Electric System.

Our work supports registered entities, including Generator Owners and Operators, Transmission Owners and Operators, Reliability Coordinators, Balancing Authorities, and Distribution Providers. We work across NERC Reliability Standards, FERC orders, RTO/ISO market participation rules, Regional Entity oversight, and state regulatory frameworks.

We do this work differently than larger consulting firms. Engagements are overseen by a senior practitioner with regulator-side experience. We don't staff for billable hours; we staff for outcomes. Our deliverables are written to be operationally executable and audit-defensible, not to manufacture activity. Where automation can replace manual work, we build the automation. Where senior judgment is required, the senior is in the room.

Our services are written to be clearly defensible: operationally executable in real time and audit-defensible at compliance review. Every deliverable is structured for the auditor's question, not the consultant's binder. Energy Compliance services include, but are not limited to:

- NERC reliability and compliance advisory support
- Reliability governance and program assessments
- Registration and applicability analysis

- Operational and engineering reliability alignment
- Compliance program design and improvement
- Audit and enforcement support (non-advocacy)
- Mitigation planning and Self-Report development
- Training and executive briefings on reliability frameworks
- Regulator-perspective program reviews
- NERC compliance: program support, interpretation, and audit preparation
- Senior advisory: direct engagement on complex reliability questions
- Industry engagement: standards development and working-group participation
- Audit defense: Notice of Penalty response and settlement posture

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

Energy Compliance, Inc. partners with registered entities on the institutional and technical questions that define strong reliability and cybersecurity programs, from classification through audit through enforcement response.

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, Rules of Procedure, Appendix 4C, Compliance Monitoring and Enforcement Program (effective May 19, 2022), Sections 4.5 (Self-Reports), 4.5A (Self-Logging), 4.8 (Preliminary Screen), 4.1.3.1 (scope of Compliance Audits), 4A.1 (Compliance Exception Process), 4A.2 (FFT Process) and 6.1 through 6.4 (Mitigation Plans). https://www.nerc.com/globalassets/who-we-are/rules-of-procedure/appendix-4c.pdf
- North American Electric Reliability Corporation, Rules of Procedure, Appendix 4B, Sanction Guidelines of the North American Electric Reliability Corporation (effective January 19, 2021), Section 3.3 aggravating and mitigating factors, footnotes 6 through 8, Section 3.4 and the Aggravating and Mitigating Factors table. https://www.nerc.com/globalassets/who-we-are/rules-of-procedure/appendix-4b.pdf
- North American Electric Reliability Corporation, Rules of Procedure, Appendix 2, Definitions Used in the Rules of Procedure (effective June 27, 2024), definitions of Alleged Violation, Compliance Enforcement Authority, Compliance Exception, Find, Fix, Track and Report, Inherent Risk Assessment, Mitigating Activities, Mitigation Plan, Notice of Penalty, Preliminary Screen, Self-Logging and Self-Report. https://www.nerc.com/globalassets/who-we-are/rules-of-procedure/appendix-2.pdf
- North American Electric Reliability Corporation, ORCP and CMEP Annual Report (February 11, 2026), covering calendar year 2025: Noncompliance Discovery Methods, Disposition of Noncompliance, Mitigation of Noncompliance, Compliance History, and Self-Report and Mitigation Training. https://www.nerc.com/globalassets/programs/enforcement/cmep-and-vegetation-reports/2025-orcp-and-cmep-annual-report.pdf

© Energy Compliance, Inc. · EC-WP-603 · October 2026