CYBERSECURITY · CIP SERIES · EC-WP-204

CIP Misclassification: Detection & Correction

Why CIP-002 categorization errors persist, how audit teams find them, and how to correct them for good.

Every CIP obligation follows from the categorization an entity makes under CIP-002, so an error there spreads into every standard that comes after it. This reference explains where categorization goes wrong, how audit teams reconstruct it, and how to correct an error and build a program that stays accurate. It reflects the requirements in force in October 2026 and the CIP-002-8 changes that take effect July 1, 2028.

Disclaimer & Legal Notice

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

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

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

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

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

Foreword

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

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

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

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

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

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

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

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

Executive Summary

CIP-002 categorization errors keep showing up in NERC enforcement. NERC's 2025 annual report lists CIP-002 among the ten most frequently reported CIP noncompliance areas. In my view, that count understates the problem. When an entity fails to identify an Electronic Access Control or Monitoring System, a Physical Access Control System, or a Protected Cyber Asset, the ERO Enterprise processes the failure as a single CIP-010 R1 violation, not as a CIP-002 violation. Some scoping error never carries a CIP-002 label at all.

The same report says registered entities self-identified about 85% of reported noncompliance in 2025. Most noncompliance, then, is found by the entity itself. In my view, misclassification comes from process, from incomplete asset visibility, and from decisions made once and never revisited, and rarely from bad intent.

This reference covers six points:

- **Classification is not a one-time exercise.** CIP-002 R2 requires a review at least once every 15 calendar months, not when something changes. That trigger has to come from the entity's own program.
- **A wrong rating reaches back.** A misclassification determination raises every requirement that should have applied during the period. Two years of wrong scope means two years of control gaps.
- **Errors cluster.** They gather around Control Center boundaries, the 1,500 MW generation criterion, the weighted-value substation test, the 15-minute functional test, and associated systems.
- **Auditors reconstruct your categorization** from your registration, the facility, your architecture, and the systems named in your evidence.
- **Disclosure timing changes the posture.** The Sanction Guidelines give self-reporting credit for a Self-Report made promptly and before a compliance monitoring engagement detects the problem. A notification letter for an upcoming engagement generally ends that eligibility for in-scope requirements.
- **The goal is continuous accuracy** in an operating environment that doesn't pause for compliance.

The requirements are also moving. CIP-002-8, approved by FERC on March 19, 2026, takes effect July 1, 2028, with a revised Control Center definition and a new threshold for Transmission Operator and Transmission Owner Control Centers. Categorizations built today should be checked against both versions.

1 Why Misclassification Keeps Happening

To understand why misclassification persists despite years of CIP enforcement and extensive industry guidance, you have to understand the conditions under which classification decisions get made. Classification is an ongoing obligation performed against a changing operational environment. The processes most entities use to meet that obligation were not designed for continuous accuracy.

The standard's own drafters saw the risk. The rationale for CIP-002 R2 states that "the miscategorization or non-categorization of a BES Cyber System can lead to the application of inadequate or non-existent cyber security controls." That is the whole problem in one sentence.

1.1 The Point-in-Time Trap

Most entities perform CIP-002 identification and categorization during a defined window, typically the periodic review or a response to a known change, and then treat the resulting lists as authoritative until the next scheduled review. The weakness is plain. Operational environments change continuously, and a determination that was correct when made can become wrong without triggering any formal review.

A substation that did not meet a medium impact criterion at the last review may meet one today because new lines have pushed its aggregate weighted value over the threshold. A backup Control Center that was barely used may now carry real operating load after a reconfiguration. A generating plant may have been uprated. None of these changes automatically triggers a CIP-002 review under most entities' internal processes, so the categorization accumulates errors between formal review cycles.

1.2 The Legacy Decision Problem

The most consequential source of misclassification is an old decision that was correct at the time and never revisited. In entities with long operating histories, the categorization record often contains determinations made under earlier versions of the standard, by people who have since left, carried forward through successive updates without real re-evaluation.

This is where misclassification gets dangerous. Earlier versions of CIP-002 identified Critical Assets and their Critical Cyber Assets. Version 5, approved by FERC in Order No. 791 in 2013, replaced that approach with the High, Medium, and Low Impact categorization of every BES Cyber System that applies today. A determination that rests on the old vocabulary does not answer the current question. When an auditor asks for the basis of a low impact rating and the entity produces a memorandum that cites superseded standard language, the rating is, for practical purposes, undocumented under the current requirements.

1.3 The Bias Toward Under-Classification

Misclassification has a direction. In my view, entities more often rate systems lower than warranted than higher. That is not an accident. A higher rating brings more requirements, more controls, more evidence, and more audit exposure. The institutional incentives point toward the lower rating wherever the criteria leave room to argue.

The bias shows up most often as an over-reading of the standard's qualifiers and exemptions. CIP-002 contains a short list of exemptions and several criteria with narrowing language, which Chapter 2 covers. Each is specific. In practice, entities sometimes apply them broadly, excluding systems on general operational characteristics rather than on the conditions the standard actually sets. The result looks complete and defensible on its face and still leaves out assets that a careful reading would include.

1.4 Organizational Gaps That Create Blind Spots

Classification accuracy depends on visibility: the ability to identify every asset that performs a reliability function and test it against the criteria. That visibility needs input from operations, engineering, IT, and compliance. When those groups don't share an asset inventory, when systems go into service without anyone telling compliance, or when engineering changes skip a formal change assessment, the categorization develops blind spots.

The blind spots are worst in entities that have grown through acquisition, merger, or rapid build-out. Acquired assets may have been categorized under different methods or earlier versions of the standard. Facilities added to the BES through new interconnections may never have been evaluated for CIP purposes at the time they connected. The compliance team that owns the categorization may not see those assets at all.

1.5 Chapter Summary

Misclassification persists for three reasons. The operating environment is dynamic, the processes most entities use to maintain categorization are not, and the incentives favor the lower rating wherever the criteria permit argument. Fixing those conditions takes process discipline that most entities do not have by default and have to build on purpose.

> **From the Field**
>
> Misclassification is one of the most preventable problems in CIP. Programs that categorized once at registration and stopped have already drifted. Turnover, system additions, and reorganizations are the normal conditions of utility operations, and the categorization has to be designed to survive them.

2 The CIP-002 Classification Framework in Plain Terms

CIP-002 is the foundation of the CIP framework. Its rationale for R1 says the impact categories "will be the basis for the application of appropriate requirements in CIP-003-CIP-011," and later standards, including CIP-013 and the coming CIP-015, key their applicability to the same ratings. Every other CIP obligation depends on getting categorization right.

2.1 What CIP-002 Actually Requires

CIP-002-5.1a, in force since 2016, has two requirements. R1 requires a process that considers six asset types: Control Centers and backup Control Centers; transmission stations and substations; generation resources; systems and facilities critical to system restoration; Special Protection Systems; and, for Distribution Providers, specified Protection Systems. From that process the entity identifies each high impact BES Cyber System (Part 1.1), each medium impact BES Cyber System (Part 1.2), and each asset that contains a low impact BES Cyber System (Part 1.3). A discrete list of low impact systems is not required.

R2 requires the entity to review those identifications, and update them if changes are found, at least once every 15 calendar months, and to have its CIP Senior Manager or delegate approve them on the same cycle. Both obligations apply even if the entity has nothing to list.

2.2 The Identification Sequence Cannot Be Shortcut

The definitions build on each other, and the work has to follow them in order. Start with the BES assets the entity owns. Identify the Cyber Assets at those assets that meet the BES Cyber Asset definition. Group those into BES Cyber Systems by the reliability tasks they perform. Then rate each BES Cyber System against Attachment 1. Associated systems, meaning the EACMS, PACS, and Protected Cyber Assets that serve a high or medium system, inherit their obligations from that system.

Skipping steps produces errors. Entities that begin with a list of known control systems and work backward will miss Cyber Assets that were never on the list but still perform reliability functions. Entities that try to rate individual devices rather than BES Cyber Systems will misapply criteria written at the system level. The sequence is not paperwork. It is the structure that makes the result reliable.

2.3 What the Bright-Line Criteria Actually Say

Attachment 1 sorts every BES Cyber System into one of three ratings. The criteria characterize impact. The standard says they are not stand-alone compliance requirements, but R1 cannot be met without applying them.

Rating	What Attachment 1 covers (CIP-002-5.1a)
High (Section 1)	Control Centers and backup Control Centers of Reliability Coordinators; of Balancing Authorities for 3,000 MW or more of generation in a single Interconnection or for assets meeting criterion 2.3, 2.6, or 2.9; of Transmission Operators for assets meeting criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10; and of Generator Operators for assets meeting criterion 2.1, 2.3, 2.6, or 2.9
Medium (Section 2)	Generation of 1,500 MW or more at a single plant location (2.1); reactive resources of 1,000 MVAR or more (2.2); generation the Planning Coordinator or Transmission Planner designates (2.3); Transmission Facilities at 500 kV or higher (2.4); 200 to 499 kV stations over an aggregate weighted value of 3,000 (2.5); IROL-critical facilities (2.6); Nuclear Plant Interface Requirements (2.7); generation interconnection for 2.1 or 2.3 plants (2.8); SPS and RAS that affect IROLs (2.9); automatic load shedding of 300 MW or more (2.10); and Control Centers not rated high for Generator Operators at 1,500 MW or more (2.11), Transmission Operators (2.12), and Balancing Authorities at 1,500 MW or more (2.13)
Low (Section 3)	BES Cyber Systems not rated high or medium that are associated with a Control Center, a transmission station or substation, a generation resource, a restoration facility, a Special Protection System, or a Distribution Provider Protection System within the standard's applicability

Two things stand out. High impact reaches only Control Centers and backup Control Centers, and that includes Generator Operator Control Centers. Backup Control Centers are not a lesser category; they appear in the same criteria as the primary. And the high impact criteria leave little room for judgment, while the medium impact criteria carry conditional language that creates more room for interpretation and more room for error.

Low impact is the residual tier. The standard's Background section says BES Cyber Systems at Facilities not included in criteria 1.1 to 1.4 and 2.1 to 2.11 "default to be low impact." My advice is to treat a low impact rating as a conclusion you can defend in writing, not as the place systems land when nobody looked closely. Entities that do that approach the whole exercise more carefully.

2.4 Exemptions and Qualifiers: Narrow by Design

CIP-002-5.1a contains four exemptions in Section 4.2.3: Cyber Assets at facilities regulated by the Canadian Nuclear Safety Commission; Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters; systems regulated by the Nuclear Regulatory Commission under a cyber security plan under 10 C.F.R. 73.54; and, for Distribution Providers, systems and equipment outside the specified Protection Systems. That is the whole list. There is no general exemption for systems whose operational role seems limited.

Several criteria also carry narrowing language. Criterion 2.1 says that for each group of generating units, "the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW." Criterion 2.2 does the same for reactive resources. Read that language carelessly in one direction and you put every unit controller in medium scope. Read it carelessly in the other and you miss the shared system that ties the units together.

Auditors who examine the basis for a low impact rating will check whether the entity claimed an exemption or qualifier it did not meet. The test is the text of the standard, not the entity's sense of how much a system matters.

2.5 What Changes on July 1, 2028

Two sets of revisions take effect on the same day. The Project 2016-02 virtualization revisions, approved by FERC in Docket No. RM24-8-000, revise the BES Cyber Asset definition and other CIP terms to cover Virtual Cyber Assets. CIP-002-8, approved by FERC on March 19, 2026, in Docket No. RD25-8-000, revises the Control Center definition so it also reaches a Transmission Owner facility that can control transmission Facilities at two or more locations in real time using SCADA. It also rewrites criterion 2.12 to rate each Transmission Operator or Transmission Owner Control Center and backup Control Center by an aggregate weighted value of the BES Transmission Lines it monitors and controls, with medium impact for values exceeding 6,000, subject to an exclusion for local systems that mainly serve load. Where the revised 2.12 raises a categorization, the implementation plan allows 24 months from the CIP-002-8 effective date.

CIP-002-7, the virtualization version of the standard, is retired immediately before CIP-002-8 takes effect, so entities move from CIP-002-5.1a to CIP-002-8. Any categorization review done between now and then should note which determinations the new Control Center definition and the new criterion 2.12 could change.

2.6 Chapter Summary

CIP-002 is precise where entities most often want flexibility, and it leaves judgment where entities most often want a bright line. The identification sequence has to be followed in order. The high impact criteria are close to mechanical. The medium impact criteria need careful reading of specific language. The exemptions and qualifiers are narrow and cannot be stretched to cover systems that do not meet their conditions.

> **From the Field**
>
> CIP-002 is the standard everything else hangs from. Get the categorization wrong and the whole program is misaligned. The sequence is identify, group, then rate, and programs that compress it make their errors at the boundaries.

3 Where Entities Get Classification Wrong

In my view, classification errors are not spread evenly across the criteria. They cluster around specific provisions, specific system types, and specific organizational conditions. Knowing where categorization breaks down is the first step toward preventing it.

3.1 The Control Center Boundary Problem

Control Centers are the most clearly defined high impact assets in CIP-002, yet the boundary of what counts as the Control Center is often drawn too tightly. The NERC Glossary defines a Control Center as one or more facilities hosting operating personnel that monitor and control the BES in real time to perform the reliability tasks of a Reliability Coordinator, Balancing Authority, Transmission Operator for transmission Facilities at two or more locations, or Generator Operator for generation Facilities at two or more locations, "including their associated data centers."

That last phrase matters. The Control Center is not just the operations floor and the screens the operators watch. The question for each Cyber Asset that supports the floor, whether a historian, a real-time analysis tool, or a system feeding situational awareness to the operators, is the functional test in the BES Cyber Asset definition. Entities that categorize the SCADA front end and the energy management system but leave out supporting systems because they are "IT, not OT" are misclassifying by scope exclusion. The one place the standard draws a line on communications is the exemption for communication networks and data links between discrete Electronic Security Perimeters. That exemption is specific. It is not a general carve-out for anything that moves data.

The Generator Operator piece catches fleet operators. A remote operations center whose operators monitor and control generation Facilities at two or more locations in real time to perform Generator Operator reliability tasks meets the Control Center definition. Under criterion 2.11, if it performs Generator Operator obligations for an aggregate highest rated net Real Power capability of 1,500 MW or more in a single Interconnection over the preceding 12 calendar months, its BES Cyber Systems are medium impact. That total grows site by site as a fleet is added, and the rating changes when the fleet crosses the line, not when someone next looks.

3.2 Generation: The Aggregation Trap

Criterion 2.1 rates generation by "each group of generating units at a single plant location," with an aggregate highest rated net Real Power capability of the preceding 12 calendar months of 1,500 MW or more in a single Interconnection. The threshold is a plant-level aggregate. An

entity that evaluates each unit on its own will under-rate the shared systems that manage the plant as a whole.

Criterion 2.8 extends the reach. Transmission Facilities, including generation interconnection Facilities, that would cause the loss of a plant identified under criterion 2.1 or 2.3 bring their BES Cyber Systems into medium impact too. A generation owner who rates the plant correctly and forgets the interconnection has finished only half the job.

A related error is categorizing the generating unit rather than the cyber systems. CIP-002 categorizes BES Cyber Systems, the programmable electronic devices that perform reliability tasks, not the physical generation asset. The turbine or the inverter block as physical equipment is not what CIP-002 rates. The programmable controls in it, and the control system that manages its output for the Generator Operator, may well be.

Newly registered Category 2 inverter-based resource Generator Owners and Generator Operators should track one more document. NERC's compliance dates document for them (Revision 1.5, August 4, 2026) lists CIP-002 through CIP-013 and CIP-015 as "requires modification" before they become applicable to Category 2 IBRs. Watch that list rather than assume CIP applies, or doesn't.

3.3 Transmission Substations: Configuration Complexity

Transmission categorization depends on configuration. Criterion 2.4 covers Transmission Facilities at 500 kV or higher. Criterion 2.5 covers stations operating between 200 kV and 499 kV that connect at 200 kV or higher to three or more other stations and exceed an aggregate weighted value of 3,000. Each incoming and outgoing BES Transmission Line to another station adds 700 points at 200 to 299 kV and 1,300 points at 300 to 499 kV. Lines at 500 kV and above add zero; criterion 2.4 covers those facilities on its own.

That arithmetic is where engineering and compliance disconnects create the most exposure. Compliance may hold a categorization built from the station configuration at the last review. Engineering may since have added a line, moved a termination, or reconfigured a bus. One new 345 kV line can move a station over 3,000. If nobody tells compliance and nobody re-runs the calculation, the categorization goes wrong without anyone making a deliberate error.

3.4 The "It's Not BES" Assumption

One of the most consequential patterns is the blanket assumption that a system is not a BES Cyber Asset because it sits at a distribution-voltage facility, belongs to IT rather than operations, or carries a "business system" label. None of those facts decides the question. The definition does. A BES Cyber Asset is a Cyber Asset that, if rendered unavailable, degraded, or misused, would within 15 minutes of its required operation, misoperation, or non-operation adversely impact one or more Facilities, systems, or equipment that would affect the reliable operation of the BES. Redundancy of the affected Facilities may not be considered.

That functional test catches systems that organizational categories miss. A historian that aggregates real-time data from multiple substations and feeds the Control Center may not look like a BES Cyber Asset from an IT desk. If its loss would degrade the operators' situational

awareness enough to affect their real-time management of the BES within 15 minutes, it may well be one. Categorization starts with function, not with location or label.

3.5 Associated Systems: The Error That Shows Up Elsewhere

No current CIP standard has a stand-alone requirement to identify EACMS, PACS, or Protected Cyber Assets. NERC's 2025 annual report explains that when an entity misses one, the ERO Enterprise rolls the resulting noncompliance into a single CIP-010 R1 violation and documents the other missed requirements in its description. NERC calls that a temporary practice pending a standards fix, and on October 15, 2025, the Standards Committee authorized drafting under Project 2021-03 to centralize identification of those systems.

The practical point is simple. An authentication server, a badge system, or a networked device inside the Electronic Security Perimeter that nobody identified is a categorization failure, even though the violation may carry a CIP-010 number.

3.6 Chapter Summary

Classification errors cluster around Control Center boundaries, generation aggregation, substation weighted values, the 15-minute functional test, and associated systems. In each area the failure is the same: applying a simpler rule than the standard requires, either because the specific language is not well understood or because the people doing the categorization lack the operational information to apply it.

> **From the Field**
>
> Knowing where the errors cluster is how you prevent them. The BES Cyber Asset definition carries operational logic that an asset inventory alone can't surface. And a categorization done by a vendor and never reviewed by the registered entity is a categorization waiting to be wrong.

4 How Auditors Identify Misclassification

Audit teams do not take an entity's categorization at face value. They approach it with investigative techniques built to surface both the error itself and the conditions that produce it. Knowing those techniques lets an entity find its own exposure before the audit team does.

4.1 The Registration Cross-Reference

Every registered entity appears on the NERC Compliance Registry for the functions it performs. Audit teams compare the CIP-002 lists against that registration. If an entity is registered as a Transmission Operator with Control Centers and with stations that meet a medium impact criterion, and those assets do not appear on its lists at the right rating, the gap is obvious.

This cross-reference catches a common pattern: entities with accurate registrations that never connected their registration to their categorization. The registration tells the audit team what functions the entity performs. The CIP-002 lists should reflect the systems that support those functions. The gaps between the two are where categorization questions start.

4.2 The Facility Walk and the Inventory

In on-site audits, the audit team can walk the facility, see which systems are present, what they connect to, and how they are configured, and compare that against the categorization, the Electronic Security Perimeter documentation, and the baselines. Systems in the room but not on the list, connections in the network but not in the diagrams, and configurations that differ from documented baselines all generate questions.

This technique is especially good at surfacing the scope exclusion errors described in Chapter 3. An auditor who sees a historian rack in a Control Center and notes that it does not appear in the ESP documentation or the asset list will ask why it was left out. If the answer is "we considered it an IT system," the auditor will test the system against the BES Cyber Asset definition no matter how the entity labels it internally.

4.3 Pattern Recognition Across the Evidence Package

Experienced auditors read evidence packages as narratives, not checklists. CIP-007 patch management evidence names specific systems. CIP-005 evidence describes specific network architectures. CIP-010 baseline evidence documents specific Cyber Assets. When those streams describe different populations of systems, the discrepancy signals a categorization or scoping problem.

This approach catches misclassification that no single requirement's evidence would reveal. An entity whose ESP documentation and patch records cover different sets of systems is

presenting evidence of an inconsistency. The audit team will resolve it by asking which population is correct and then testing the systems that appear in one stream but not the other.

4.4 The Self-Report as Evidence of Program Maturity

When an entity self-reports a categorization error, the Self-Report itself becomes evidence of how mature its CIP program is. Appendix 4C of the NERC Rules of Procedure says a Self-Report will include a risk assessment, a description of the extent of the noncompliance, its cause, and the actions taken or planned to mitigate it, including preventing recurrence. A Self-Report that delivers each of those clearly reads very differently from one that is vague about scope, unsure of the exposure period, and thin on corrective action.

Reviewers will look at whether the corrective actions reach the root cause, the process failure that allowed the error, or only the error itself. Fixing the one misclassified system without fixing the process that produced it signals that the same failure may be producing other errors nobody has found yet.

4.5 Chapter Summary

Audit teams find misclassification by comparing registration against categorization, observing the facility, reading the evidence package for inconsistent populations, and judging the quality of any Self-Report. Entities that want to find misclassification first should apply the same techniques to their own programs, starting with the registration cross-reference. It requires no technical investigation and consistently surfaces the most consequential gaps.

> **From the Field**
>
> The audit team will reconstruct your categorization from your asset inventory, your architecture, and the operational descriptions you provided. They look for what categorization documentation usually misses: undocumented control paths, dual-purpose assets, and changes that never reached the lists. The pattern is reproducible, so self-audit against it before they arrive.

5 Correction Strategy: Reclassification Without Panic

Discovering a misclassification, whether through internal review, a third-party assessment, or audit preparation, starts a sequence of decisions that will shape both the compliance outcome and the enforcement exposure. How an entity manages the correction matters as much as the correction itself.

5.1 Scope the Exposure Quickly and Completely

The first step is to scope the exposure precisely. Determine when the misclassification began: not when it was discovered, but when the system should first have carried the higher rating. Identify every CIP requirement that should have applied during that period and was not implemented. Then assess whether those gaps left systems unprotected in ways that matter to the risk assessment.

Scoping does two jobs. It defines the content of a Self-Report, and it defines the corrective action scope. An entity that discloses before it understands the exposure may learn during enforcement that the problem is bigger than its disclosure said. In my view, that does more damage to the entity's credibility with the Regional Entity than an initially larger but complete disclosure.

Scoping cannot become a reason to wait. The Sanction Guidelines say an entity should submit a Self-Report "as soon as practical, but typically within three months of discovery," and provide more complete information as it becomes known. Scope fast, report inside that window, and supplement.

5.2 Self-Reporting: The Decision and the Timing

Appendix 4C encourages Self-Reports at the time an entity becomes aware that it has, or may have, violated a Reliability Standard. Appendix 4B, the Sanction Guidelines, treats self-reporting as a mitigating factor. NERC or the Regional Entity considers whether the entity reported within a reasonably prompt time after becoming aware of the violation and before detection by a compliance monitoring engagement, along with any mitigating activities the entity undertook voluntarily.

Timing has a hard edge. Under the Sanction Guidelines, receipt of a notification letter for an upcoming Compliance Audit, Spot Check, or Self-Certification generally ends the entity's eligibility for self-reporting credit for the requirements in scope of that engagement until it ends. A categorization error found during audit preparation, after the letter has arrived, is a different conversation from one found during a routine internal review.

For entities approved for Self-Logging, Appendix 4C allows minimal-risk noncompliance to be logged for later review instead of self-reported, with a rebuttable presumption that it will be resolved as a Compliance Exception. A categorization error that left real systems unprotected will rarely be minimal risk.

The Self-Report and every written submission after it become part of the enforcement record. The Regional Entity reviews them, NERC may review them, and if the matter ends in a Notice of Penalty, NERC files that notice with FERC.

5.3 Corrective Actions That Actually Correct

The most common failure in misclassification corrective actions is treating the symptom rather than the cause. An entity that re-rates the affected system and implements the missing controls has fixed the immediate problem. If it has not fixed what allowed the error, whether a gap in change assessment, a disconnect between engineering and compliance, or the absence of a real periodic review, the same failure will produce the next misclassification.

The CMEP builds that expectation in. Under Appendix 4C, a Mitigation Plan must describe the activities to correct the noncompliance, to correct its cause, and to prevent recurrence. Corrective actions that show systemic process change, such as a redesigned change assessment workflow, a formal categorization review schedule, or defined communication between engineering and compliance, present a very different picture from corrective actions that only install missing controls on one system.

5.4 Chapter Summary

Correcting a misclassification takes precision at every step: scoping the full exposure quickly, reporting inside the window with a Self-Report that states the scope and the fix accurately, and implementing corrective actions that reach the root cause. Entities that treat this sequence as an obligation to minimize will find that the enforcement process probes exactly the parts they handled most casually.

> **From the Field**
>
> A misclassification you surface yourself is a different conversation from one an audit team surfaces. Start with scope: what's wrong, how it affected the program, and which controls were missed. Move quickly, because the self-reporting window is real. A correction that is fast but wrong gets corrected again at the next audit, with worse exposure.

6 Building a Classification Program That Stays Accurate

The goal is not to classify correctly once. It is to keep the categorization accurate in an operating environment that changes faster than compliance processes usually adapt. That takes deliberate program design. More documentation of the same process will not do it. Different processes, built for continuous accuracy rather than point-in-time completeness, will.

6.1 The Change Assessment Process Is the Core Control

The most important single control in a categorization program is a change assessment that evaluates every material operational change for CIP-002 implications before the change goes in. That is the mechanism that catches configuration changes, capacity additions, and system modifications that would otherwise create undiscovered misclassifications between reviews.

To work, the assessment has to live inside the operational change management workflow, not run beside it as a parallel compliance activity. Changes are approved through change management. The CIP-002 assessment should be a defined step in that approval, not a separate review afterward. When the assessment is part of change approval, it happens on every change. When it is a separate process, it happens on the changes someone remembered to send to compliance.

6.2 Planned and Unplanned Changes

NERC's implementation plans distinguish two kinds of change. The plan approved with CIP-002-8 describes a planned change as one the entity planned and implemented, such as an automation upgrade that installs Cyber Assets meeting Attachment 1 at a substation. The new BES Cyber System must comply upon commissioning. An unplanned change happens outside the entity's control, such as a transmission line built or retired elsewhere, or a plant modified to change its rated output, so that an unchanged system becomes medium impact. For unplanned changes, the plan allows 12 months to comply after the new categorization, and 24 months for an entity identifying its first high or medium impact BES Cyber System.

In my view, two lessons follow. First, a planned change carries no grace period, which is exactly why the change assessment in Section 6.1 has to happen before commissioning. Second, those timelines exist for changes. A system that met the criteria all along and was simply missed was not the subject of a change, and an entity should not expect the unplanned-change clock to cover it.

6.3 The Periodic Categorization Review

Section 2.1 sets out the R2 cycle. In practice, the periodic review is often the only one that occurs, so changes with categorization consequences can sit unexamined for more than a year.

A defensible periodic review does more than confirm the existing lists. It tests them against current configurations, re-runs the arithmetic for criteria such as 2.1, 2.5, and 2.11, cross-references the lists against the entity's registration, and checks whether any change since the last review affects a determination. It means going out and looking at the operating environment, not just re-reading last year's documentation.

6.4 Governance: Who Owns Classification

Categorization accuracy is shared between compliance and the operations and engineering groups that can see the systems being rated. When that sharing is not formalized, when nobody owns the lists, there is no escalation path for categorization questions, and nobody is accountable for telling compliance about operational changes, the categorization drifts.

Mature programs assign ownership explicitly: a compliance owner for the CIP-002 lists, named operations and engineering contacts responsible for reporting relevant changes, and a governance path for resolving categorization questions between reviews. That structure does not eliminate errors. It creates the conditions under which errors are found and corrected before they accumulate into enforcement exposure.

6.5 Chapter Summary

A categorization program that stays accurate is an operational process built into how the entity manages its facilities and systems. The change assessment catches misclassification at the moment it would otherwise be created. The periodic review catches what got past the change assessment. Governance makes sure both actually happen. Entities with all three in place carry a very different categorization risk than entities that rely on the 15-month review alone.

> **From the Field**
>
> Put the CIP-002 question inside change approval, re-run the numbers at every review, and give the lists an owner. Those three habits do more for categorization accuracy than any amount of documentation.

Glossary

Term	Meaning in this paper
BES Cyber Asset	A Cyber Asset that, if rendered unavailable, degraded, or misused, would within 15 minutes of its required operation, misoperation, or non-operation adversely impact one or more Facilities, systems, or equipment which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the BES. Redundancy of affected Facilities may not be considered. The 15 minutes is not a grace period; it defines the functional test. The definition revised for virtualization, effective July 1, 2028, adds Virtual Cyber Assets.
BES Cyber System	One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity. CIP-002 rates systems, not individual devices.
Bright-Line Criteria	The impact rating criteria in CIP-002 Attachment 1. They are objective thresholds and conditions. The entity applies them; it does not weigh them.
Categorization (Classification)	The process under CIP-002 R1 of identifying high and medium impact BES Cyber Systems and the assets that contain low impact BES Cyber Systems. This reference uses "classification" and "categorization" interchangeably.
Change Assessment	An entity's own process for evaluating a proposed operational or system change for CIP-002 consequences before it is implemented. CIP-002 does not require one by name; in this reference's view it is the primary control against drift.
CIP Senior Manager	The single senior management official with overall authority and responsibility for leading and managing implementation of, and continuing adherence to, CIP-002 through CIP-011. Approves the CIP-002 identifications at least once every 15 calendar months.
Compliance Monitoring and Enforcement Program (CMEP)	The program, set out in Appendix 4C of the NERC Rules of Procedure, through which NERC and the Regional Entities monitor, assess, and enforce compliance with Reliability Standards.
Control Center	One or more facilities hosting operating personnel that monitor and control the BES in real time to perform the reliability tasks, including their associated data centers, of a Reliability Coordinator, a Balancing Authority, a Transmission Operator for transmission Facilities at two or more locations, or a Generator Operator for generation Facilities at two or more locations. The definition effective July 1, 2028, adds certain Transmission Owner facilities that control transmission Facilities at two or more locations using SCADA.
Exemption	One of the four categories of Cyber Assets and systems that Section 4.2.3 of CIP-002-5.1a exempts from the standard. Exemptions apply only when their stated conditions are met.

Term	Meaning in this paper
High Impact BES Cyber System	A BES Cyber System used by and located at a Control Center or backup Control Center that meets Attachment 1, Section 1: Reliability Coordinator Control Centers, and Balancing Authority, Transmission Operator, and Generator Operator Control Centers that meet the stated conditions.
Misclassification	A BES Cyber System rated at the wrong impact level, or not identified at all. Most often, a system rated low that should have been medium or high. The standard's own rationale calls it miscategorization. This is a working term, not a NERC Glossary term.
Mitigation Plan	The plan a Registered Entity submits under Appendix 4C, Section 6, describing how it will correct the noncompliance, correct its cause, and prevent recurrence.
Periodic Review	The CIP-002 R2 obligation to review the R1 identifications, and update them if changes are found, at least once every 15 calendar months, with CIP Senior Manager or delegate approval.
Planned and Unplanned Changes	Implementation plan terms for changes that raise a categorization. A planned change must comply upon commissioning. An unplanned change gets defined compliance timelines, generally 12 months.
Self-Logging	A program under Appendix 4C, Section 4.5A, that lets eligible entities log minimal-risk noncompliance for later review instead of submitting a Self-Report.
Self-Report	A Registered Entity's disclosure of a possible or actual violation to its Compliance Enforcement Authority, including a risk assessment, the extent and cause of the noncompliance, and the mitigating actions. Self-reporting is a mitigating factor under the Sanction Guidelines when it is prompt and comes before detection by a compliance monitoring engagement.

How Energy Compliance Can Help

Misclassification is a process problem, and process problems are what we fix. Energy Compliance classification advisory services include:

- CIP-002 asset identification and classification reviews
- Classification inventory gap analysis and correction support
- Change assessment process design and integration
- Self-report preparation and enforcement response support
- Mock audit preparation with classification focus
- Periodic classification review facilitation

Around that core, EC provides CIP classification work covering inventory review, gap analysis, self-report support, and correction strategy; audit defense with Notice of Penalty response and settlement posture; NERC compliance program support, interpretation, and audit preparation; senior advisory on complex reliability and enforcement questions; and industry engagement in standards development and working-group participation. Services are tailored to the functional role, system impact, and regulatory posture of each organization, and our CIP-focused services are listed in About Energy Compliance, Inc.

WattOps Compliance is EC's NERC compliance evidence platform (wattopscompliance.com). A categorization error often surfaces when one evidence stream names systems another doesn't, and WattOps keeps the evidence behind your other NERC obligations in one place. EC will run one standard at one facility through WattOps at no cost (CIP standards excluded).

RenewOps is EC's renewable operations monitoring and analytics platform, with a Data Center module. For fleet operators, the operations systems that monitor sites at two or more locations are where Control Center and criterion 2.11 questions start.

Start with your CIP-002 lists. If you cannot explain every rating, and every system you left off, in writing, call us.

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

Phone: 763.438.4427

About the Author

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

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

Education:

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

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

About Energy Compliance, Inc.

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

We support Generator Owners and Operators, Transmission Owners and Operators, Reliability Coordinators, Balancing Authorities, and Distribution Providers. A senior practitioner with regulator-side experience oversees every engagement. We staff for outcomes, not billable hours. Where automation can replace manual work, we build it. Where senior judgment is required, the senior is in the room.

Our CIP-focused services include, but are not limited to:

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

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

- NERC, Reliability Standard CIP-002-5.1a, Cyber Security: BES Cyber System Categorization, including Attachment 1, Impact Rating Criteria (effective December 27, 2016). https://www.nerc.com/globalassets/standards/reliability-standards/cip/cip-002-5.1a.pdf
- NERC, Reliability Standard CIP-002-8, Cyber Security: BES Cyber System Categorization (effective July 1, 2028). https://www.nerc.com/globalassets/standards/reliability-standards/cip/cip-002-8.pdf
- NERC, Reliability Standards: CIP standards listing with status and effective dates. https://www.nerc.com/standards/reliability-standards/cip
- NERC, Project 2021-03, Implementation Plan for CIP-002-8 (August 29, 2024). https://nerc.com/pa/Stand/Project202103_CIP002_Transmission_Owner_Control_Ce/2021-03_Implementation_Plan_08292024.pdf
- NERC, Glossary of Terms Used in NERC Reliability Standards. https://www.nerc.com/glossary-of-terms
- NERC, Rules of Procedure, Appendix 4B, Sanction Guidelines (eff. Jan. 19, 2021). https://www.nerc.com/globalassets/who-we-are/rules-of-procedure/appendix-4b.pdf
- NERC, Rules of Procedure, Appendix 4C, CMEP (effective May 19, 2022). https://www.nerc.com/globalassets/who-we-are/rules-of-procedure/appendix-4c.pdf
- NERC, ORCP and CMEP Annual Report (February 11, 2026). https://www.nerc.com/globalassets/programs/enforcement/cmep-and-vegetation-reports/2025-orcp-and-cmep-annual-report.pdf
- NERC, Reliability Standards Compliance Dates for GOs and GOPs, IBR Registration Initiative Supplemental (Revision 1.5, August 4, 2026). https://nerc.com/pa/Stand/202401%20Rules%20of%20Procedure%20Definitions%20Alignment%20GO/ComplianceDatesforGOs_GOPS.pdf
- Federal Energy Regulatory Commission (FERC), Order Approving Reliability Standard CIP-002-8, Docket No. RD25-8-000 (March 19, 2026), 91 FR 14013. https://www.govinfo.gov/content/pkg/FR-2026-03-24/pdf/2026-05715.pdf
- FERC, Order No. 919, Virtualization Reliability Standards, Docket No. RM24-8-000 (March 19, 2026), 91 FR 13957. https://www.govinfo.gov/content/pkg/FR-2026-03-24/pdf/2026-05716.pdf
- FERC, Order No. 791, Version 5 Critical Infrastructure Protection Reliability Standards, Docket No. RM13-5-000 (November 22, 2013), 78 FR 72756. https://www.govinfo.gov/content/pkg/FR-2013-12-03/pdf/2013-28628.pdf

© Energy Compliance, Inc. · EC-WP-204 · October 2026