



CROSSROADS • ISSUE 2 • MAY 15, 2026 • ~20 MIN READ

# Low Impact ≠ Low Risk: Why the BES Cyber System Tier Designed to Be Light Is Becoming the Hardest to Defend

1. The label was always about reliability, not security
2. What the standard actually requires of Low Impact
3. What the regulators are actually finding
4. What the public data shows
5. The aggregation problem
6. Where this is heading
7. Three observations CIP Sentinel takes from the public record
8. Sources

## The label was always about reliability, not security

Under the NERC [Critical Infrastructure Protection](#)<sup>1</sup> reliability standards, every BES Cyber System a Functional Entity owns is categorized as High, Medium, or Low Impact using the criteria in [CIP-002-5.1a Attachment 1](#)<sup>2</sup>. Generation facilities aggregated below 1,500 MW, transmission stations and substations below the operating-voltage and weighted-value thresholds in criteria 2.4 and 2.5, and most distributed energy resources individually all fall to Low Impact by default. The criteria are written around the grid's ability to absorb the loss of the facility — a Low Impact designation reflects a determination that the failure or compromise of that one facility would not, by itself, produce a measurable adverse effect on the bulk-power system within the 15-minute reliability window.

That is a reliability judgment, not a security one. As Anirban “Sunny” Ghosh, NERC CIP lead for global industrial cybersecurity at Black & Veatch, wrote in [Utility Dive on May 14, 2026](#)<sup>3</sup>: NERC CIP “low impact” is a reliability term, not a security risk rating. The designation was never intended to represent low cyber risk. The grid was built to handle an outage at one major facility; the model assumed that if a single small plant went offline, the system would compensate, and that remained manageable. Ghosh's framing of the modern problem is direct: that classification has not changed, but the world around it has. “Low impact” still describes what happens when one facility goes offline. It does not describe what happens when several do.

The compliance scoping in CIP picked up that reliability framing and gave it security-adjacent consequences. Low Impact entities are explicitly excluded from the discrete-inventory obligation of CIP-002 R1, P1.3, and from large swaths of CIP-005 (Electronic Security Perimeters), CIP-006 (Physical Security), CIP-007 (System Security Management), CIP-009 (Recovery), CIP-010 (Configuration Change Management and Vulnerability Assessments), and CIP-011 (Information Protection). For nearly the entire CIP catalog, the Low Impact obligation is a single requirement: CIP-003 R2 and its Attachment 1.



That carve-out is reasonable in isolation. The full CIP control set was sized for assets whose failure could meaningfully destabilize the BES, and applying that set to every solar inverter behind a 20 MW interconnection would be neither proportional nor administrable. But the carve-out has a second-order effect that the standard was never designed to police: it telegraphs to the rest of the organization — operations, IT, procurement, third-party vendors — that the Low Impact site is a lower-priority security environment. The compliance carve-out becomes a cultural carve-out, and the cultural carve-out becomes an attack surface.

### What the standard actually requires of Low Impact

CIP-003 R2 hangs on Attachment 1, which lists the security plan elements every Responsible Entity with assets containing Low Impact BES Cyber Systems must document and implement. Through CIP-003-8, Attachment 1 contained five sections. CIP-003-9 — which became [officially enforceable on April 1, 2026](#)<sup>4</sup> under the Supply Chain Low-Impact Revisions — added a sixth.

The current Attachment 1, post-CIP-003-9, looks like this:

| Section | Topic                                             | What the standard requires                                                                                                         |
|---------|---------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| 1       | Cyber Security Awareness                          | Reinforce cyber security practices at least once every 15 calendar months                                                          |
| 2       | Physical Security Controls                        | Control physical access to BES Cyber Systems and locations of low impact BES Cyber Asset connectivity                              |
| 3       | Electronic Access Controls                        | Permit only necessary inbound and outbound electronic access, and authenticate all Dial-up Connectivity where technically feasible |
| 4       | Cyber Security Incident Response                  | Document and implement an incident response plan; test the plan at least once every 36 calendar months                             |
| 5       | Transient Cyber Asset and Removable Media         | Mitigate the risk of malicious code introduction from Transient Cyber Assets and Removable Media                                   |
| 6 NEW   | Vendor Electronic Remote Access Security Controls | Added under CIP-003-9: determine, disable, and detect malicious communications for vendor electronic remote access                 |

Six sections does not sound like a heavy regime. Read them together with the existing CIP-002 inventory carve-out and CIP-003's note that "an inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required," and the compliance footprint looks lighter still: a Low Impact entity is not required to produce a discrete asset list, is not required to baseline configurations, is not required to perform vulnerability assessments, is not required to retain 90 days of logs or review them at 15-day intervals, and is not required to enforce 15-month password change cycles.

The ERO Enterprise has been clear in its own published guidance that these carve-outs do not excuse the underlying security obligation. From the 2024 ReliabilityFirst [CIP Themes and Lessons Learned report](#)<sup>5</sup>: "The ERO Enterprise acknowledges that CIP-002.5.1a R1, P1.3 states that 'a discrete list of low impact BES Cyber Systems is not required,' and a note in the current version of CIP-003 R2 provides that 'an inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required.' But these statements do not excuse entities' obligations to protect those systems and assets under CIP-003 R2. Indeed, it may be very difficult to achieve the security objectives of CIP-003 R2 without



such inventories and lists, so entities should strongly consider developing and maintaining them.”

CIP-003-9’s new Section 6 closes one of the most-discussed gaps in the prior version. The 2023 [Holland & Knight summary](#)<sup>6</sup> of the FERC approval order described the new obligation as requiring Responsible Entities to include vendor electronic remote access security controls in their cybersecurity policies, and to have methods for determining that vendor remote access exists, disabling it when necessary, and detecting malicious communications through it — a three-verb framework that recognizes that Low Impact assets can serve as conduits to attacks on other assets, or facilitate reconnaissance into the broader environment, when security-in-depth is not applied across the supply chain. NERC’s own data, cited by [ABS Group’s primer on CIP-003-9](#)<sup>7</sup>, came from evaluating more than 1,000 entities and found that uncontrolled third-party remote access into Low Impact sites — equipment manufacturers, managed service providers, and other non-registered parties — was widespread, often operating outside any enforceable security baseline.

CIP-003-9 is not the end of the regulatory trajectory. On March 19, 2026, FERC unanimously approved [CIP-003-11](#)<sup>8</sup> as part of the broader Virtualization Reliability Standards package, with additional changes to Electronic Access Controls for Low Impact BES Cyber Systems on top of the CIP-003-9 baseline. The package is heavy in absolute terms: 11 modified CIP Standards, four new definitions to the NERC Glossary, and 18 modified definitions. CIP-003-11’s implementation timeline tracks the broader virtualization rollout — meaningful enforcement on Low Impact entities lands in the April 2028 horizon, with continuous monitoring and automated audit trails described in industry guidance as the 2030 maturity expectation.

Layered on that is FERC [Order 887](#)<sup>9</sup>, issued January 19, 2023, which directed NERC to develop Internal Network Security Monitoring requirements for High Impact BES Cyber Systems and Medium Impact systems with External Routable Connectivity — and which simultaneously directed NERC to submit a feasibility study on extending INSM to Low Impact BES Cyber Systems and Medium Impact systems without External Routable Connectivity. The Order’s text explicitly contemplates that extending INSM to “at least a subset of low impact BES Cyber Systems in the future could be necessary to protect the security and reliability of the Bulk-Power System.” The study is the regulatory hinge: it is how Low Impact internal monitoring becomes a future requirement rather than a recommendation.

## What the regulators are actually finding

The regulators have not been quiet about what they see when they audit Low Impact programs. The 2024 ReliabilityFirst Themes report opens by naming four enterprise-wide trends: latent vulnerabilities, insufficient commitment to low impact CIP programs, shortages of labor and skillsets, and performance drift. The ordering matters: Low Impact is the second of four named themes across the entire CIP enforcement landscape, not a footnote to it.

The report’s framing of the Low Impact problem is direct. From page 9: “In a vacuum, individual assets containing low impact BES Cyber Systems may not pose a significant risk to the overall BES. Nevertheless, compromise of such assets could create localized issues, and an individual low impact asset could (a) serve as a channel to attack other assets or (b) be used to conduct reconnaissance. And the potential risk to the BES multiplies in scenarios where several low impact assets are compromised in a coordinated attack.”

The volume trend matches the framing. Between 2017 and 2023, the ERO Enterprise processed a steadily increasing volume of noncompliances with CIP-003 R2. ReliabilityFirst’s report does not project the trend will reverse, citing three reasons: violation intake and inventory remain at high levels, the number of entities with Low Impact assets continues to grow (in part due to the ongoing registration of



inverter-based resources), and new requirements like the CIP-003-9 vendor electronic remote access obligation raise the bar further on what the program must demonstrate.

The specific cases the regulators have published are instructive — not because any one case is exceptional, but because the failure patterns repeat:

- An entity's process required completion of a form and the capture of evidence demonstrating that a Transient Cyber Asset had been scanned for malicious code prior to each use. The entity confirmed that TCAs had been used, but could not locate a single completed form and had no evidence of scanning for malicious code prior to use.
- Another entity could not identify how many TCAs were in use, let alone provide evidence showing management of those TCAs to reduce the risk of introducing malicious code in the environment.
- Experienced staff at Low Impact sites were observed remotely unlocking doors for unauthorized individuals, neglecting to secure doors and manage keys, and failing to identify a need to create or apply security plans to new sites — or to sites transitioning from medium/high to low impact.
- In one case in the broader 2024 enforcement record, more than 100 administrators had unauthorized access to BCSi repositories for over eight years.

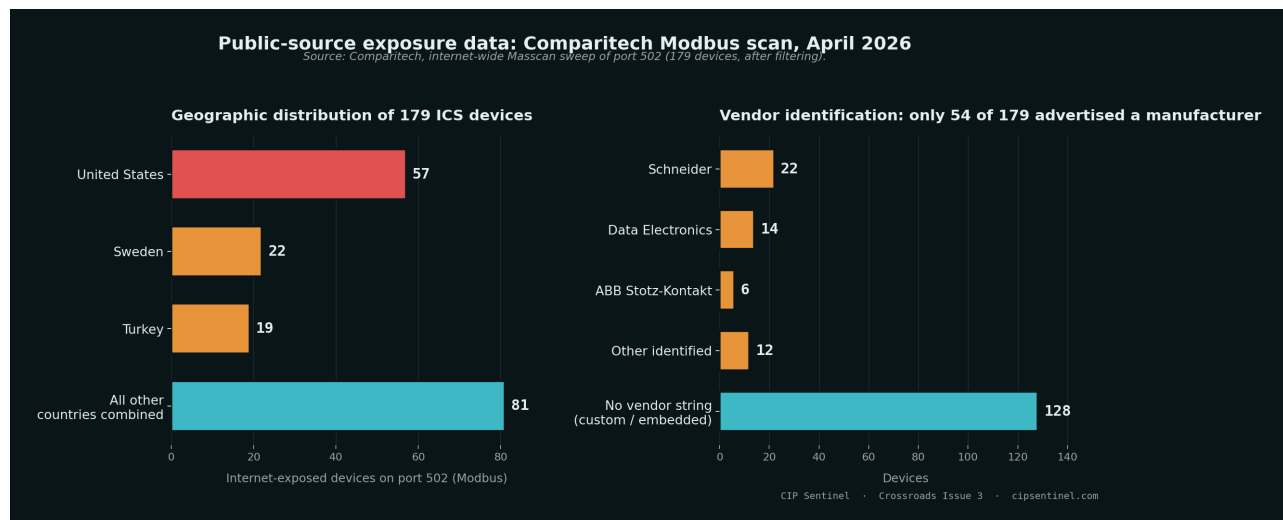
The October 2025 FERC [Lessons Learned from Commission-Led CIP Reliability Audits](#)<sup>10</sup> zeroes in on a different failure mode that is structural rather than cultural: third-party oversight at Low Impact sites. Under the report's "Use of Third Parties to Perform Reliability Standards Compliance Duties" finding, FERC staff observed that one audited entity did not perform oversight of a task it contracted to a third party. The entity had contracted with the third party to ensure that all firewall rules were up to date and necessary; the third party did not complete the task, leaving unnecessary inbound and outbound electronic access within the entity's firewall — inconsistent with CIP-003-8 Attachment 1, Section 3 (Electronic Access Controls). The registered entity lacked oversight controls and only identified the gap on a delayed, after-the-fact follow-up.

FERC's conclusion in that finding is worth quoting in full because it sets the responsibility allocation clearly: "Registered entities are ultimately responsible for compliance with the applicable Reliability Standards, even when using third parties for their compliance obligations." Entities should document and track the security and compliance risks of outsourcing functions to third parties in their supply chain risk management plan, and should implement compensating controls — Service Level Agreements, internal monitoring and alerting of third-party actions, geographic restrictions on third-party staff, infrastructure, and data — to reduce the compliance and security risk of using vendors.

The cultural dimension is the part that does not show up cleanly in any single audit. ReliabilityFirst's diagnosis: "Root causes in these cases often point to ineffective training and lack of direction or guidance, which can result in staff treating low impact sites as functionally out of scope for NERC CIP purposes, which in turn can increase the frequency of less-than-desirable security decisions." The compliance carve-out at the standard level becomes an attention carve-out at the operations level — and that attention deficit is what audits keep finding.

### What the public data shows

The audit record is one source of evidence. The internet itself is another. In April 2026, Comparitech researcher Mantas Sasnauskas published [the results of an internet-wide Masscan sweep of port 502](#)<sup>11</sup>, the default Modbus port. Of 311 responses initially received, the team filtered out emulation software, cloud-based devices, and devices with wildly fluctuating readings unlikely to mirror real-world outputs, leaving 179 responses with a high likelihood of coming from real ICS devices.



Two-panel chart showing geographic distribution of 179 internet-exposed Modbus devices (US 57, Sweden 22, Turkey 19, other 81) and vendor identification (Schneider 22, Data Electronics 14, ABB Stotz-Kontakt 6, other identified 12, no vendor string 128).

The geographic distribution of those 179 devices skewed sharply toward the United States: 57 in the U.S., 22 in Sweden, 19 in Turkey, and 81 distributed across all other countries. Of the 179 devices, 128 exposed only firmware versions or internal IDs without a manufacturer string — a fingerprint typical of custom controllers or embedded modules. The 54 devices that did advertise their manufacturer broke down with Schneider Electric leading at 22 devices, Data Electronics at 14, and ABB Stotz-Kontakt at 6. Named device models found in the open included Schneider TM221CE40T and BMXP342020 logic controllers, the Fastwel CPM713 logic controller, the eGauge Core EG4015 energy meter and data logger, and the A.Eberle PQI-DA-SMART voltage and power logger. The functional spread was deliberate: logic controllers that drive outputs from sensor inputs, energy meters that log circuit-level consumption, and grid-performance monitors. The report flagged one device as part of a national railway network, and two — one in Asia, one in Europe — as part of their respective countries' national power grid infrastructure.

The exposure mechanics were what made the finding notable. As [Industrial Cyber summarized](#)<sup>12</sup> on April 10, 2026, Modbus is a decades-old protocol that lacks encryption and does not require authentication. Revealing a device's make and model allows an attacker to look up the associated register list — the manufacturer-published table that maps each of the device's holding registers to its underlying sensor reading (temperature, pressure, voltage, current, flow) or control state (switch, motor, pump, controller target, error code). And because Modbus does not require authentication, an attacker who can read holding registers can also write to them. In Comparitech's words, even minor unauthorized changes could disrupt the system that depends on the device's readings. Researcher Justin Schamotta, framing the report's headline conclusion: "Without proper safeguards such as firewalls, VPNs, network segmentation, and secure authentication, internet-exposed ICS devices make easy targets."

It is reasonable to ask how directly the 179-device dataset maps to NERC's Low Impact universe. The Comparitech scan did not classify devices by NERC Functional Entity status, and the dataset crosses sectors — manufacturing, transportation, water, and energy. It is fair to assume that some fraction of the U.S. devices are owned by NERC-registered entities and some are not, and that some fraction of those that are registered are running Low Impact assets. What the dataset does establish, independent of CIP scoping, is that internet-exposed Modbus devices controlling real industrial processes are findable, identifiable, and writable in non-trivial numbers — a finding that becomes harder to dismiss when read alongside the audit pattern of Low Impact entities with incomplete network diagrams, unscanned



Transient Cyber Assets, and unmonitored vendor remote access.

The threat-actor side of the public record is equally direct. In December 2024 and again in 2025, joint advisories from CISA, the FBI, the NSA, and partner agencies described [Volt Typhoon's](#)<sup>13</sup> prepositioning in U.S. critical infrastructure networks — energy, water, transportation, and communications. The International Institute for Strategic Studies, in a February 2026 Cyber Power Matrix post, summarized the trajectory: “Originally believed to be pursuing espionage objectives, Volt Typhoon’s activities are now widely regarded as an effort by the Chinese government to preposition on critical infrastructure targets in preparation for disruption operations in the event of a military crisis with the US.” Public reporting through Q1 2026 placed Volt Typhoon’s confirmed dwell time in some U.S. critical infrastructure environments at five years or more.

Volt Typhoon’s targeting pattern — Living off the Land techniques, low-and-slow persistence, abuse of legitimate administrative protocols — is one for which High and Medium Impact CIP controls (CIP-005 ESPs, CIP-007 R4 logging and 15-day reviews, CIP-010 R3 vulnerability assessments) are designed precisely to detect. Those controls do not apply at Low Impact. CIP-003 Attachment 1 Section 4 requires an incident response plan tested every 36 months. It does not require continuous logging, 90-day log retention, 15-day log reviews, or the alerting on logging failure that CIP-007 R4 imposes at Medium and High. Five-year dwell time and 36-month incident-response-plan testing intervals are dimensions of the same problem.

Salt Typhoon is the second half of the same story. The PRC-linked group that breached major U.S. telecommunications carriers in 2024 was, per FBI public statements in February 2026, [still very much ongoing](#)<sup>14</sup> as a threat. Trend Micro’s [Q1 2026 U.S. public sector threat report](#)<sup>15</sup> noted Salt Typhoon’s expansion into congressional email penetration on January 9, 2026. Salt Typhoon’s footprint is communications-focused, but the actor profile — long dwell, multi-target campaigns, infrastructure repurposing — generalizes to the same Low Impact exposure surface that Volt Typhoon exercised on the energy side.

The Iranian campaign against U.S. water and energy sites is the third public data point and possibly the most operationally illustrative. On April 7, 2026, the EPA, FBI, CISA, and NSA issued a [joint advisory](#)<sup>16</sup> warning that Iranian-affiliated threat actors had exploited internet-facing devices at U.S. critical infrastructure sites — including water, energy, and municipal locations. The vector was an authentication bypass vulnerability in Rockwell Automation Logix controllers; the attacks involved malicious interactions with project files, leading to data manipulation visible on both the HMI and the SCADA displays. The advisory urged operators to enable multifactor authentication, remove devices from the public internet, check logs for suspicious activity, and place physical-mode switches on Rockwell devices to the “run” position. The federal agencies did not specify the number or specific locations of the attacks but noted the incidents resulted in financial losses and operational disruption.

The pattern across all three actor sets is consistent: the attacks did not target the largest, best-resourced, highest-classified facilities. They targeted the smaller ones — the ones operating with less mandatory monitoring, less mandatory logging, fewer mandatory access controls, and often less internal capacity to detect or respond. The Low Impact tier is where that asymmetry lives in the CIP catalog.



## The aggregation problem

The defense against the “Low Impact is not low risk” framing has long been the impact analysis baked into CIP-002. The premise: if a single facility’s loss does not affect the BES, then the cybersecurity controls for that facility do not need to scale to BES-protection levels. That premise was reasonable when the grid was characterized by a small number of large generation facilities, when distributed energy resources were not registered, and when adversaries were not running multi-target prepositioning campaigns.

Three structural shifts have stressed the premise.

The first is the changing generation mix. ReliabilityFirst’s 2024 report flagged the trend explicitly: “the number of entities with low impact assets will continue to grow (e.g., ongoing efforts relating to registration of inverter-based resources).” Inverter-based resources — utility-scale solar, wind, battery storage — are increasingly registered as Low Impact under the existing thresholds. Each individual interconnection sits comfortably below the 1,500 MW aggregate single-site threshold that triggers Medium Impact rating. But the operating model for these resources is, by construction, distributed: hundreds or thousands of installations, often managed remotely through cloud-connected vendor platforms, contributing together to the same balancing area’s generation mix.

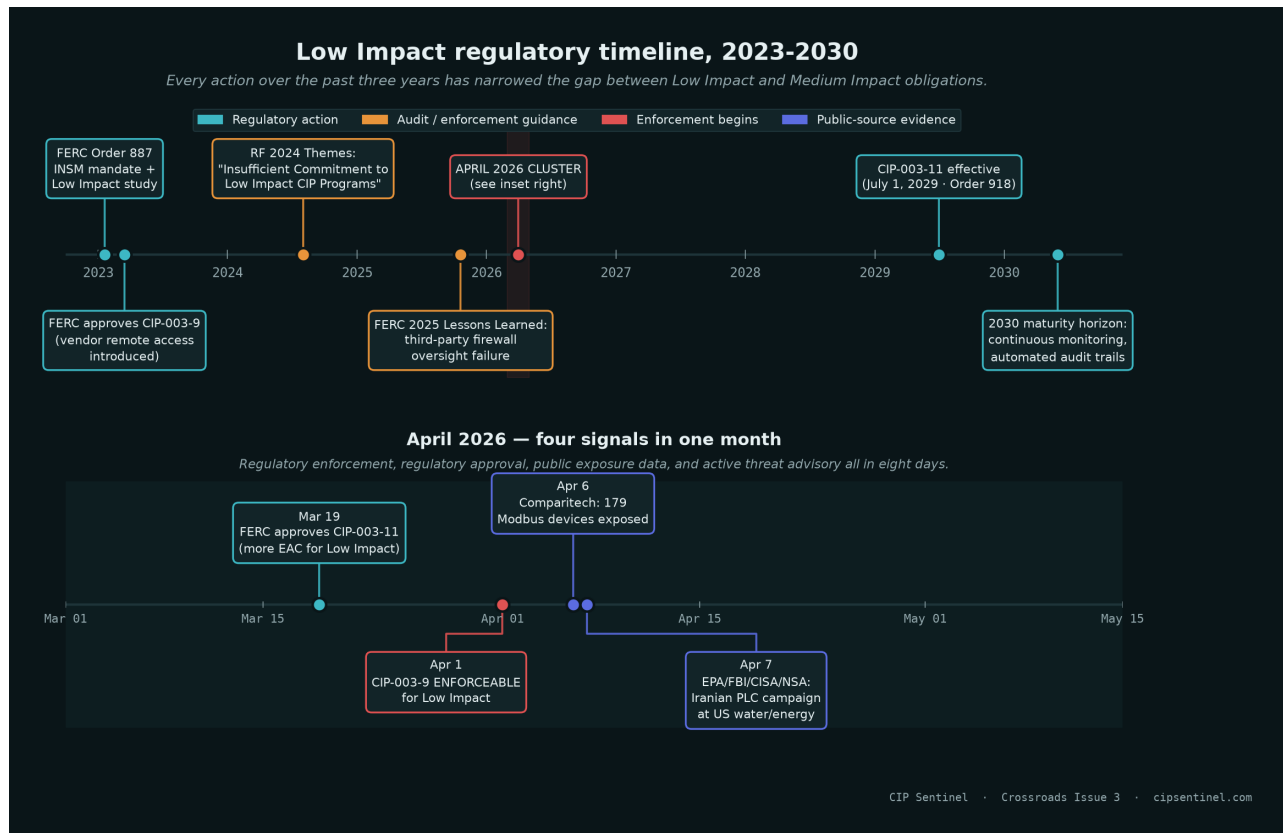
The second is the changing failure mode. The traditional grid was built to tolerate the loss of a single major facility through automatic protection actions — relays disconnecting affected lines, generators picking up displaced load. That design did not contemplate the simultaneous loss of many smaller resources. The May 4, 2026 NERC Level 3 Alert on large computational loads — 1,000+ megawatts dropping off the bulk-power system in seconds during repeated events — was a non-cyber example of how rapid simultaneous loss of multiple smaller assets can stress system stability. A coordinated cyber attack that simultaneously degraded a fleet of Low Impact inverters, or a population of Low Impact distribution-connected generators, would produce a different version of the same waveform.

The third is the changing adversary. Volt Typhoon, Salt Typhoon, and the Iranian Rockwell-PLC campaign are not single-target operations. They are fleet operations, designed for parallelism, optimized for dwell. The economic model is unfavorable to the defender: an attacker who has compromised one Low Impact site has, in many cases, simultaneously compromised a template that maps to dozens of similar sites with similar configurations, similar vendor relationships, and similar exposure surfaces.

Ghosh, in the Utility Dive piece, captures the framing in two consecutive sentences: “‘Low impact’ still describes what happens when one facility goes offline. It does not describe what happens when several do.” The same sentence pair could be written about cybersecurity rather than reliability: the CIP-002 categorization is built around the single-asset compromise, and the realistic attack scenario is no longer single-asset.

## Where this is heading

The regulatory direction over the past three years is consistent and the trajectory is clear, even if the cadence is slow. Tracing the major Low Impact actions:



Low Impact regulatory timeline 2023-2030 showing FERC Order 887 INSM mandate and Low Impact study (Jan 2023), CIP-003-9 approval introducing vendor remote access controls (Mar 2023), ReliabilityFirst 2024 Themes naming insufficient commitment to Low Impact as one of four enterprise audit themes (Aug 2024), FERC 2025 Lessons Learned on third-party firewall oversight failure (Oct 2025), the April 2026 cluster (CIP-003-11 approval, CIP-003-9 enforcement begins, Comparitech publishes 179-device Modbus exposure report, EPA/FBI/CISA/NSA Iranian PLC campaign advisory), CIP-003-11 effective date (Jul 2029), and 2030 maturity horizon.

The slope of that timeline is what matters more than any single line item. Every major regulatory action over the past three years has narrowed the gap between Low Impact and Medium Impact obligations. None has widened it. CIP-003-9 introduced the first concept that Medium and High already had — controlled vendor remote access. CIP-003-11 layered on additional Electronic Access Control language. Order 887's INSM study is the foundation for a future requirement that would put the first network-monitoring obligation on Low Impact entities.

A parallel signal sits outside the CIP catalog: the [Rural and Municipal Utility Cybersecurity Program](#)<sup>17</sup>, a \$250 million federal program running through fiscal year 2026, exists explicitly because small, often Low-Impact-only utilities need outside support to close the same gaps that ReliabilityFirst's audit themes describe. Kenergy CEO Tim Lindahl's December 2025 congressional testimony urging reauthorization framed the same problem from the operator side: the smallest utilities cannot, on their own budgets and staffing, close the gap that the threat environment is now opening.

The two regulatory tracks — the CIP standards on one side, the federal cybersecurity programs on the other — are converging on the same conclusion. The Low Impact tier of CIP cannot remain as light as it has historically been, because the threat picture, the asset mix, and the public exposure data have all moved.



### Three observations CIP Sentinel takes from the public record

This issue is commentary, and it is built entirely from the public record cited above. CIP Sentinel does not have access to non-public audit findings, registered-entity compliance evidence, or threat intelligence outside what federal agencies and independent researchers have published. What follows is independent analysis only — three observations the public sources permit, framed in the language CIP Sentinel uses throughout this publication.

One: the absence of an inventory obligation does not produce the absence of inventory risk. The public ERO record from 2017 through 2023 describes a steady accumulation of CIP-003 R2 noncompliances grounded in entities that did not know what they had. The FERC October 2025 lessons learned describes the same pattern from a different angle: an entity that contracted out a firewall task to a third party and could not detect that the third party had not done it. Public guidance from the ERO Enterprise commonly emphasizes that achieving the security objectives of CIP-003 R2 is “very difficult” without inventories and discrete identification of Low Impact BES Cyber Systems, even though the standard does not require either. The standard’s choice to exempt inventory from the mandatory evidence list is not a comment on whether the inventory is needed for security; it is a comment on what the standard chose to make auditable. The two are different decisions.

Two: vendor electronic remote access at Low Impact was the gap most loudly telegraphed by the public record before CIP-003-9 closed it. NERC’s evaluation of 1,000+ entities found uncontrolled third-party remote access into Low Impact sites was widespread. The April 2026 enforcement of CIP-003-9 closes the regulatory side of that gap, but the operational side persists at every site where the vendor catalog is unclear, where remote access methods have proliferated organically over years, and where the “determine, disable, detect” three-verb framework has not been mapped onto specific vendor agreements. Public reporting describes Volt Typhoon and similar actors as effective at exploiting precisely this kind of legitimate, lightly-tracked access path; reporting on the Iranian Rockwell campaign emphasized that the affected devices were directly internet-facing and that “remove devices from the public internet” was among the federal agencies’ first recommendations.

Three: aggregation risk is now a public-record concept, not an internal one. The pre-2023 framing of Low Impact built around single-asset failure has been overtaken by public statements from NERC, ReliabilityFirst, and independent industry analysis describing the multiplicative risk of coordinated compromise across many small assets. The ReliabilityFirst report says it plainly: “the potential risk to the BES multiplies in scenarios where several low impact assets are compromised in a coordinated attack.” That is no longer a theoretical concern documented only inside audit reports — it is the publicly stated rationale for the regulatory trajectory of the past three years and the publicly described targeting pattern of the threat actors of greatest concern in the same window.

None of this is a recommendation that Low Impact entities apply Medium Impact controls. The standard’s tiering was designed to be proportional, and the proportionality is what makes it administrable across the more than 1,500 NERC-registered Functional Entities. What the public record does suggest is that the floor written into CIP-003 R2 is, by its own architects’ description, a floor — and that the most credible Low Impact programs are the ones already treating their CIP-003 Attachment 1 obligations as the beginning of a security program rather than the entirety of one.

The standard is moving in that direction. The threat picture is moving faster than the standard. The gap between the two is where Low Impact programs are now operating, and the public sources reviewed in this issue all describe that gap as widening before it narrows.



## Sources

- Anirban “Sunny” Ghosh, “Security beyond CIP: When ‘low impact’ doesn’t mean low risk,”<sup>3</sup> Utility Dive, May 14, 2026.
- Anna Ribeiro, “Internet-exposed ICS devices running insecure Modbus leave critical infrastructure open to disruption, Comparitech finds,”<sup>12</sup> Industrial Cyber, April 10, 2026.
- Comparitech, “Critical Infrastructure at Risk: 179 ICS Devices Exposed Online,”<sup>11</sup> April 6, 2026.
- GDS Associates, “FERC unanimously approves sweeping sets of CIP standards,”<sup>8</sup> March 23, 2026.
- Tenable, “Prepare for NERC CIP-003-9 Compliance: 2026 Deadlines and Requirements,”<sup>4</sup> March 17, 2026.
- FERC, “Lessons Learned from Commission-Led CIP Reliability Audits,”<sup>10</sup> October 20, 2025.
- ReliabilityFirst, “2024 CIP Themes and Lessons Learned,”<sup>5</sup> August 2024.
- Holland & Knight, “FERC Approves New Cybersecurity Standards for Low-Impact Electric Assets,”<sup>6</sup> March 17, 2023.
- ABS Group, “A Primer on NERC CIP-003-9: Supply Chain Security Risk for Low Impact BES Cyber Systems.”<sup>7</sup>
- John Bruce / IISS, “IISS notes Volt Typhoon’s targeting of US infrastructure signals disruptive intent beyond espionage,”<sup>13</sup> Industrial Cyber, February 9, 2026.
- Trend Micro, “U.S. Public Sector Under Siege: Threat Intelligence for Q1 2026,”<sup>15</sup> April 9, 2026.
- EPA, “EPA, FBI, CISA, NSA Issue Joint Cybersecurity Advisory to Water System Regarding Iranian-Affiliated Cyber Attacks,”<sup>16</sup> April 7, 2026.
- Cybersecurity Dive, “Iran-linked hackers target water, energy in US, FBI and CISA warn,”<sup>18</sup> April 8, 2026.
- Utility Dive, “China seeks long-term vulnerabilities in US energy systems,”<sup>17</sup> December 3, 2025.
- CyberScoop, “FBI: Threats from Salt Typhoon are ‘still very much ongoing,’”<sup>14</sup> February 19, 2026.
- NERC, Critical Infrastructure Protection (CIP) Reliability Standards.<sup>1</sup>
- NERC, CIP-002-5.1a, Attachment 1.<sup>2</sup>
- FERC, “Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems” (Order 887),<sup>9</sup> February 9, 2023.

## Sources & references

1. Critical Infrastructure Protection  
<https://www.nerc.com/standards/reliability-standards/cip>
2. CIP-002-5.1a Attachment 1  
<https://www.nerc.com/globalassets/standards/reliability-standards/cip/cip-002-5.1a.pdf>
3. Utility Dive on May 14, 2026  
<https://www.utilitydive.com/news/when-low-impact-doesnt-mean-low-risk-cyber-nerc/819730/>
4. officially enforceable on April 1, 2026  
<https://www.tenable.com/blog/prepare-nerc-cip-003-9-compliance-deadlines-2026>
5. CIP Themes and Lessons Learned report  
<https://www.rfirst.org/wp-content/uploads/2024/08/2024-CIP-Themes-and-Lessons-Learned.pdf>
6. Holland & Knight summary  
<https://www.hklaw.com/en/insights/publications/2023/03/ferc-approves-new-cybersecurity-standards-for-low-impact-electric>



7. ABS Group's primer on CIP-003-9  
<https://www.abs-group.com/Knowledge-Center/Insights/A-Primer-on-NERC-CIP-003-9-Supply-Chain-Security-Risk-for-Low-Impact-BES-Cyber-Systems/>
8. CIP-003-11  
<https://www.gdsassociates.com/ferc-unanimously-approves-sweeping-sets-of-cip-standards/>
9. Order 887  
<https://www.federalregister.gov/documents/2023/02/09/2023-01453/internal-network-security-monitoring-for-high-and-medium-impact-bulk-electric-system-cyber-systems>
10. Lessons Learned from Commission-Led CIP Reliability Audits  
[https://www.ferc.gov/sites/default/files/2025-10/25\\_Lessons%20Learned\\_1014%201.pdf](https://www.ferc.gov/sites/default/files/2025-10/25_Lessons%20Learned_1014%201.pdf)
11. the results of an internet-wide Masscan sweep of port 502  
<https://www.comparitech.com/news/critical-infrastructure-at-risk-179-ics-devices-exposed-online/>
12. Industrial Cyber summarized  
<https://industrialcyber.co/industrial-cyber-attacks/internet-exposed-ics-devices-running-insecure-modbus-leave-critical-infrastructure-open-to-disruption-comparitech-finds/>
13. Volt Typhoon's  
<https://industrialcyber.co/industrial-cyber-attacks/iiss-notes-volt-typhoons-targeting-of-us-infrastructure-signals-disruptive-intent-beyond-espionage/>
14. still very much ongoing  
<https://cyberscoop.com/fbi-salt-typhoon-ongoing-threat-cybertalks-2026/>
15. Q1 2026 U.S. public sector threat report  
[https://www.trendmicro.com/en\\_us/research/26/d/us-public-sector-under-siege.html](https://www.trendmicro.com/en_us/research/26/d/us-public-sector-under-siege.html)
16. joint advisory  
<https://www.epa.gov/newsreleases/epa-fbi-cisa-nsa-issue-joint-cybersecurity-advisory-water-system-regarding-iranian>
17. Rural and Municipal Utility Cybersecurity Program  
<https://www.utilitydive.com/news/china-energy-utility-cyber-threat-typhoon/806893/>
18. "Iran-linked hackers target water, energy in US, FBI and CISA warn,"  
<https://www.cybersecuritydive.com/news/iran-linked-hackers-targeting-water-energy-in-us-fbi-and-cisa-warn/816949/>