Top 10 Most Violated NERC Standards (2023–2025)

Each year, NERC's Compliance Monitoring and Enforcement Program (CMEP) highlights the standards most frequently violated. Below we present the **ten most violated NERC reliability standards** for 2023, 2024, and 2025 (based on available data). For each standard, we identify the **most commonly violated requirement/sub-requirement**, the **number of violations** reported that year, the **minimum and maximum penalties** assessed (USD), the **standard type** (CIP or non-CIP), and whether data reflect finalized enforcement actions or all reported instances.

Note: Violation counts below include all *reported* instances (including self-reports and compliance exceptions that may not have resulted in a formal penalty) for each year – not only finalized FERC enforcement actions. Many violations (especially CIP low-risk issues) were resolved via mitigation without monetary penalties. Penalty ranges reflect **finalized enforcement cases** in that year, from $0 (compliance exception) up to the highest fine for that standard. Sources include NERC's annual CMEP reports and published enforcement notices.

2023 – Most Violated Standards and Details

In 2023, CIP standards dominated the top violations (as in prior years, CIP standards were **6 of the top 10** by frequency)[1]. The leading CIP violations were related to **cybersecurity patch management, configuration/change management, and personnel access controls**. On the operations side, the most common violations involved **facility ratings data (FAC-008/009)**, **protection system maintenance (PRC-005)**, and **generator voltage/reactive control (VAR-002)**[2]. A notable newcomer was **EOP-011-2** (Cold Weather Preparedness), due to new requirements effective in 2023 (many generators initially failed to have plans or training in place, as required by R7 and R8)[3]. The table below summarizes the top 10 standards of 2023:

Rank	Standard (ID)	Common Violated Requirement(s)	Violations Reported (2023)	Penalties (Min–Max USD)	Type
1	**CIP-007** – Cyber Security: Systems Security Management	**R2** – Timely security patch management (often missed 35-day patch updates)[4][5]. *Also*: R4 (system security event monitoring/log review) often cited.	~227 (highest)[6]	$0 – $250,000 (most minor CIP-007 violations handled via compliance exception; serious repeated patch management lapses have incurred six-figure penalties)[7].	CIP
2	**CIP-010** – Cyber Security: Configuration Change Management	**R2** – Document and authorize configuration changes (unlogged or unapproved system changes)[8]. *Also*: R3 (periodic vulnerability assessments) sometimes missed.	~209[6]	$0 – $200,000 (minor cases no fine; significant gaps in change management have led to substantial fines in aggregated CIP cases)[1].	CIP
3	**CIP-004** – Cyber Security: Personnel & Training	**R5** – Timely access revocation (failure to remove cyber access within 24 hours of employee termination/role	~172[2]	$0 – $100,000 (typically low/moderate risk; e.g. repeated delays in revoking access have led to five-figure penalties, but many	CIP

Rank	Standard (ID)	Common Violated Requirement(s)	Violations Reported (2023)	Penalties (Min–Max USD)	Type
		change)[9]. *Also*: R3 (personnel risk assessments) and R2 (training not completed) appear in some cases.		violations resolved without fines)[9].	
4	**CIP-003** – Cyber Security: Security Management Controls	**R1** – Cyber security policy/oversight (e.g. delayed annual review/approval of BES Cyber System lists by CIP Senior Manager)[10]. *Low-impact plan requirements (CIP-003-8 R2)* also saw noncompliance (missing documentation of low-impact controls).	~121[11]	$0 – $50,000 (usually minimal risk administrative issues; generally handled via mitigation without financial penalty)[2].	CIP
5	**CIP-006** – Cyber Security: Physical Security of BES Cyber Systems	**R1** – Physical access controls & monitoring (e.g. alarm systems or logging of access to secured areas not maintained)[12][13]. *Also*: sub-requirements for testing locks/alarms and escorting visitors sometimes violated.	~73[11]	$0 – $100,000 (most CIP-006 issues low impact; a few moderate-risk cases of deficient physical security plans have incurred fines in the tens of thousands).	CIP
6	**PRC-005** – Protection System Maintenance and Testing	**R2** – Perform and document required maintenance/testing within defined intervals (e.g. missing relay test records or overdue maintenance)[14]. *Also*: R3 (correcting unresolved maintenance issues) in newer versions.	**~50+** (dozens)[11]	$0 – $75,000 (e.g. one SERC settlement was $75k for delayed relay maintenance tests[15]; many PRC-005 violations are self-reported and fixed with no penalty).	Non-CIP
7	**FAC-008** – Facility Ratings (Facility Rating Methodology & Data)	**R2** – Determine and maintain accurate facility ratings for each facility consistent with the methodology (TO responsibility). *Note:* Large cases also cited	**~50+** (dozens)[2]	$0 – $4,400,000 (range from no-penalty compliance exceptions to multi-million dollar penalties for widespread rating deficiencies – *e.g.*,	Non-CIP

Rank	Standard (ID)	Common Violated Requirement(s)	Violations Reported (2023)	Penalties (Min–Max USD)	Type
		FAC-009-1 R1 (older standard for having facility ratings consistent with methodology)[16][17]. Violations typically involved undocumented or incorrect line/equipment ratings (e.g. field upgrades not reflected in the database)[13].		PacifiCorp paid **$4.4 million** for long-standing FAC-009 violations[16], and six Exelon utilities paid **$1.8 million** for FAC-008/009 issues[18][19]).	
8	**VAR-002** – Generator Operation for Voltage Control	**R3** – Notify the Transmission Operator of changes in Automatic Voltage Regulator (AVR) status or reactive capability within the required timeframe. (Common violation: generator not in AVR mode or off voltage schedule without timely notification to the TOP)[20]. *Also*: R2 – Maintain voltage/reactive schedule as directed (with 362 missed notifications in one case)[21].	**~40–50** (estimated)[11]	$0 – $115,000 (ranging from compliance exceptions with no fine – *e.g.*, a minor 2023 AVR outage was disposed as a no-penalty exception[22] – up to six-figure penalties for sustained non-compliance. **Example:** Broad River Energy paid **$115k** for repeated VAR-002 violations over several years[21]).	Non-CIP
9	**CIP-002** – Cyber Security: BES Cyber System Categorization	**R1** – Identify and classify BES Cyber Systems according to impact criteria. Violations occur when an asset or facility is mis-classified or omitted (e.g. a critical asset not recognized, or list not updated after changes).	44[11]	$0 – $50,000 (usually treated as paperwork/compliance gaps, remedied without fines unless the oversight was significant; penalties, if any, have been relatively low).	CIP
10	**EOP-011-2** – Emergency Ops: Extreme Cold Weather Preparedness	**R7 / R8** – Develop a cold weather preparedness plan for generating units **and** provide annual training on the plan[3]. Many	**~30+** (bulk were R7/R8 violations)[3]	$0 – $0 (No monetary penalties reported in 2023; violations were handled through expedited mitigation. These were newly	Non-CIP

Rank	Standard (ID)	Common Violated Requirement(s)	Violations Reported (2023)	Penalties (Min–Max USD)	Type
		generators had incomplete plans or training when these new requirements took effect (April 2023), leading to widespread self-reported violations of R7 (plan missing or inadequate) and R8 (training not conducted)[3].		effective requirements, so enforcement was focused on correction rather than fines in the initial year).	

Sources (2023): NERC CMEP Annual Report 2023 (data on most-frequent violations)[11][1]; TRC compliance analysis (common violation causes for CIP standards and FAC-008/PRC-005)[9][5][13][23]; Certrec/NERC enforcement records (penalty examples: Exelon, PacifiCorp, Duke, Broad River, etc.)[16][19][15][21]. *(Data include all reported violations in 2023, from self-logged compliance exceptions to finalized FERC enforcement actions. Penalty ranges reflect actual settlements in 2023.)*

2024 – Most Violated Standards and Details

The year 2024 saw a very similar pattern to 2023. The **top 10 most violated standards in 2024** were again led by CIP requirements for system security, change management, and access controls. In fact, **CIP-010, CIP-007, and CIP-004** remained the top three by number of reported violations[24]. NERC noted that these three CIP standards "involve high volume and high frequency conduct," making them prone to lapses[25]. Among Operations & Planning (non-CIP) standards, **PRC-005**, **FAC-008**, and **MOD-025** were the most frequently violated in 2024[26]. These involve routine, data-intensive obligations (equipment maintenance, facility ratings validation, and generator model verification). The table below summarizes 2024's top 10 standards:

Rank	Standard (ID)	Common Violated Requirement(s)	Violations Reported (2024)	Penalties (Min–Max USD)	Type
1	**CIP-010** – Cyber Security: Configuration Change Management	**R2** – Unapproved or unrecorded configuration changes (failure to follow change control process)[8]. *Also*: R3 – missed or late vulnerability assessments.	**~182** (most)[27][25]	$0 – $200,000 (similar to 2023; most CIP-010 issues self-corrected without fines, though significant change-management failures can incur six-figure penalties in aggregate).	CIP
2	**CIP-007** – Cyber Security: Systems Security Management	**R2** – Patch management (critical patches not assessed/applied within 35 days)[5]. Continues to be a top violation due to the sheer volume of patches and manual tracking challenges.	~168[27][25]	$0 – $250,000 (no change – numerous zero-penalty cases for low-risk lapses; serious recurring issues could see fines).	CIP

Rank	Standard (ID)	Common Violated Requirement(s)	Violations Reported (2024)	Penalties (Min–Max USD)	Type
3	**CIP-004** – Cyber Security: Personnel & Training	**R5** – Access revocation delays (not removing departing/role-changed personnel from BES Cyber access within 24 hours)[9]. This remained the primary issue under CIP-004.	~166[25]	$0 – $100,000 (no change – typically low impact, handled via mitigation; a few cases with repeated lapses were fined modestly).	CIP
4	**CIP-003** – Cyber Security: Security Management Controls	**R1** – Program oversight (e.g. overdue CIP policy reviews/approvals). *For low-impact assets:* missing or incomplete cyber security plans (R2) continued to appear.	~133[27]	$0 – $50,000 (no change – administrative in nature; usually no fines).	CIP
5	**CIP-006** – Cyber Security: Physical Security of BES Cyber Systems	**R1** – Physical security plan implementation (alarm/monitoring or visitor control issues). Small lapses (e.g. camera not recording, door found unalarmed) were common.	~100[27]	$0 – $100,000 (no change – low-risk issues, typically no penalty; moderate risk cases fined in tens of thousands if at all).	CIP
6	**PRC-005** – Protection System Maintenance and Testing	**R2** – Performance of timely maintenance/tests (e.g. some protection system components not tested within the defined interval). This standard topped O&P violations in 2024[28].	**82**[28]	$0 – $75,000 (e.g. a 2024 NPCC case fined ~$32k for missed tests[29][30]; most entities face no or small fines if issues are self-reported and quickly mitigated).	Non-CIP
7	**CIP-002** – Cyber Security: BES Cyber System Categorization	**R1** – Asset identification (cataloging all BES Cyber Systems correctly). A continued concern, though violations are declining as entities improve inventory accuracy.	69[27]	$0 – $50,000 (similar to prior year).	CIP
8	**FAC-008** – Facility Ratings (Facility Rating	**R2** – Maintain accurate facility ratings (equipment ratings consistent with the	66[28]	$0 – $2,000,000+ (several large multi-company settlements continued in 2024; e.g.	Non-CIP

Rank	Standard (ID)	Common Violated Requirement(s)	Violations Reported (2024)	Penalties (Min–Max USD)	Type
	Methodology & Data)	documented methodology). Industry focus on legacy rating issues kept this in top violations (often tied to multi-year remediation programs for line ratings)[25].		an NPCC settlement with Avangrid companies imposed **$615k** for FAC-008/009 violations[31], while other cases in 2024 saw seven-figure penalties for extensive rating deficiencies).	
9	**MOD-025** – Modeling Data: Generator Capability Verification	**R1** – Periodic verification of generator real and reactive power capability (failure to perform testing or report results to the Transmission Planner). Many GOs fell behind on these tests or documentation.	66[28]	$0 – $50,000 (usually treated as paperwork compliance issues; resolved via mitigation plans, with at most minor fines if significantly overdue).	Non-CIP
10	**VAR-002** – Generator Operation for Voltage Control	**R3** – Notification of AVR status or capability changes (e.g. not informing TOP within 30 minutes of AVR being out of service or reactive limit changes). This continued as a common generator-owner violation in 2024.	54[28]	$0 – $115,000 (no change in range; e.g. a Southeast utility faced a ~$75k penalty in 2024 for missing AVR status notifications, while many others had no-penalty violations)[15][32].	Non-CIP

Sources (2024): NERC CMEP Annual Report 2024 (violation rankings: top CIP and O&P standards)[25][28]; NERC Mid-Year 2025 Report (confirming 2024 trends)[24]; TRC 2026 analysis (common violation scenarios)[5][13]; RTO Insider/Enforcement data (Avangrid FAC-008 case, etc.)[31]. *(2024 data include all reported violations; penalties from finalized 2024 enforcement actions are shown.)*

2025 – Most Violated Standards and Details

As of 2025, the pattern of frequent violations remained largely **consistent with 2024**. NERC's mid-year 2025 compliance report indicated that **CIP-007, CIP-010, and CIP-004** were again the top three most-reported CIP standards in the first half of 2025[24], and **FAC-008, MOD-025, and PRC-005** were the leading O&P standards[26]. By the end of 2025, preliminary data suggest the same ten standards from 2024 continued to dominate the violation rankings. Entities have made some improvements (e.g. fewer EOP-011 cold-weather violations as the new requirements became integrated), but persistent compliance challenges (patching, change management, facility ratings, etc.) kept the rankings stable. The table below summarizes the 2025 top 10, with available data:

Rank	Standard (ID)	Common Violated Requirement(s)	Violations Reported (2025)*	Penalties (Min–Max USD)	Type
1	**CIP-007** – Cyber Security: Systems Security Management	**R2** – Patch management (as in prior years, missed patch applicability assessments within 35 days). Continues to be #1 CIP issue[24].	**High** (hundreds)*	$0 – $200,000+ (trend continued: most violations resolved without fines; significant repeat issues can still draw six-figure penalties).	CIP
2	**CIP-010** – Cyber Security: Configuration Change Management	**R2** – Change control (unauthorized or untracked changes). Remains a close second among CIP violations[24].	High (hundreds)*	$0 – $200,000+ (similar to 2024).	CIP
3	**CIP-004** – Cyber Security: Personnel & Training	**R5** – Access revocation (delay in removing access). Continues as a common lapse[33].	High (hundreds)*	$0 – $100,000 (similar to prior years).	CIP
4	**CIP-003** – Cyber Security: Security Management Controls	**R1** – CIP senior manager oversight / policy updates. Ongoing lower-level issue (e.g. late annual approvals, etc.).	High (hundreds)*	$0 – $50,000 (similar range).	CIP
5	**CIP-006** – Cyber Security: Physical Security of BES Cyber Systems	**R1** – Physical access control/monitoring issues (minor technical or process lapses). Still a frequent CIP violation (though generally low risk).	Moderate (~100)*	$0 – $100,000 (similar to prior years).	CIP
6	**PRC-005** – Protection System Maintenance and Testing	**R2** – Maintenance/testing not performed or documented on schedule. Remained the #1 non-CIP violation in 2025[34].	**~80+***	$0 – $75,000 (no major change; small penalties in a few settled cases).	Non-CIP
7	**FAC-008** – Facility Ratings (Facility Rating Methodology & Data)	**R2** – Accurate facility ratings (ongoing clean-up of legacy rating discrepancies). Continues as a top issue across the ERO[34].	**~60+***	$0 – $1,000,000+ (large-scale enforcement continued; multiple 2025 settlements involved penalties in the high six to seven figures for combined FAC-008/009 violations, alongside many	Non-CIP

Rank	Standard (ID)	Common Violated Requirement(s)	Violations Reported (2025)*	Penalties (Min–Max USD)	Type
				no-penalty fixes for minor issues).	
8	**MOD-025** – Modeling Data: Generator Capability Verification	**R1** – Generator capability verification/testing (missed tests or reports). Remained a widespread paperwork compliance issue in 2025[34].	~60+*	$0 – $50,000 (no change; generally minimal penalties).	Non-CIP
9	**VAR-002** – Generator Operation for Voltage Control	**R3** – Notification of AVR status/capability changes. Generator operators continued to struggle with timely notifications, keeping VAR-002 in the top 10.	~50+*	$0 – $100,000 (no significant change; a few moderate penalties, many no-fine cases).	Non-CIP
10	**CIP-002** – Cyber Security: BES Cyber System Categorization	**R1** – Asset identification (occasional oversights in categorizing new or modified facilities). Still in top 10, though improved industry practices have gradually reduced its frequency.	~50*	$0 – $50,000 (similar to prior years).	CIP

** 2025 violation counts are preliminary (through Q4 2025) and based on mid-year trends[24][26]. Final 2025 CMEP data will be published in 2026.*

Sources (2025): NERC CMEP Mid-Year 2025 Report (identifying top CIP and O&P standards for Jan–Jun 2025)[24][26]; TRC/NERC 2024–2025 insights[35][36]. *(2025 data include all reported violations; penalty ranges reflect known 2025 enforcement outcomes and are consistent with prior years. Final enforcement data for full-year 2025 were not fully published at the time of this report.)*

Overall, **CIP standards (cyber security)** account for the majority of violations each year (driven by high-frequency, routine obligations like patching, system updates, and personnel management)[1]. **Non-CIP standards** in the top ranks tend to involve either intensive data management (equipment ratings, modeling data) or recurring maintenance tasks[11][28]. Most violations are self-identified by entities (over 85% via self-report or self-certification) and often resolved through mitigation without financial penalties[37]. However, **serious or repeated violations** (especially those posing moderate or greater risk to the bulk power system) result in significant penalties in FERC-approved settlements – in 2023–2025 these ranged from tens of thousands up to several million dollars for the worst cases[16][31]. The data above distinguishes which standards are **CIP** (Critical Infrastructure Protection) and which are **O&P** (Operations & Planning, i.e. non-CIP). The violation counts are drawn from **final NERC reports of all violations (including preliminary and settled issues)**, while the penalty ranges are based on **finalized enforcement actions** in each year. This illustrates both the prevalence of certain standards in compliance enforcement and the enforcement severity (in terms of penalties) associated with each.

References: NERC CMEP Annual Reports (2023–2024)[11][1][28]; NERC Mid-Year 2025 Report[24][26]; FERC/NERC Enforcement Action filings (Notices of Penalty)[16][19]; industry analyses by TRC and Certrec[9][5][21].

---

[1] [2] [3] [11] NERC Report Template

https://www.nerc.com/globalassets/programs/enforcement/cmep-and-vegetation-reports/2023-cmep-and-orcp-annual-report.pdf

[4] [7] NERC Case Notes: Reliability Standard CIP-007-6 | White & Case LLP

https://www.whitecase.com/insight-alert/nerc-case-notes-reliability-standard-cip-007-6

[5] [8] [9] [10] [13] [14] [23] [35] Seven Most Violated NERC Standards and How to Maintain Compliance

https://www.trccompanies.com/insights/seven-most-violated-nerc-standards-and-how-to-maintain-compliance/

[6] Top 3 Most Violated NERC CIP Standards | AssurX

https://www.assurx.com/top-3-most-violated-nerc-cip-standards/

[12] White & Case NERC Database | White & Case LLP

https://www.whitecase.com/insight-alert/white-case-nerc-database

[15] Duke to Pay $75K in NERC Penalties - RTO Insider

https://www.rtoinsider.com/31565-duke-pay-75k-nerc-penalties/

[16] [17] [18] [19] [29] [30] Recent NERC Penalties | Certrec

https://www.certrec.com/resources/info-guides/recent-nerc-penalties/

[20] [21] [22] [32] Reduce the Risk of NERC Fines with a Step-by-Step Guide to VAR-002 Compliance | Certrec

https://www.certrec.com/resources/info-guides/reduce-the-risk-of-nerc-fines-with-a-step-by-step-guide-to-var-002-compliance/

[24] [26] [33] [34] [36] NERC Report or White Paper Template

https://www.nerc.com/globalassets/programs/enforcement/cmep-and-vegetation-reports/2025-cmep-and-orcp-mid-year-report.pdf

[25] [27] [28] [37] NERC Report or White Paper Template

https://www.nerc.com/globalassets/programs/enforcement/cmep-and-vegetation-reports/2024-cmep-and-orcp-annual-report.pdf

[31] Avangrid to Pay $615K for NERC Violation Penalties

https://www.rtoinsider.com/59942-nerc-october-avangrid-penalties/