cabreza

COMPLIANCE & REGULATIONS • January 2026

Regulatory Landscape Evolution in OT Security

Mapping the new compliance terrain across NIS2, TSA, MTSA, NERC CIP, and IEC 62443

EXECUTIVE SUMMARY

Colonial Pipeline changed everything. This whitepaper maps the post-2021 regulatory landscape—from NIS2's expanded scope and TSA Security Directives to MTSA cyber requirements and NERC CIP evolution—and examines whether compliance actually produces security outcomes.

The Shift

Before May 2021, OT cybersecurity regulation existed primarily in the electric sector through NERC CIP. Other critical infrastructure operated under voluntary frameworks and industry-specific guidance.

Colonial Pipeline changed everything.

The attack demonstrated what regulators had long feared: a cyber incident affecting a single company could cascade into regional infrastructure crisis. Six days of shutdown. 45% of East Coast fuel supply affected. 17 states under emergency declaration. Gas stations from Charlotte to Washington DC running dry.

Within months: TSA Security Directives for pipeline operators. Surface transportation requirements. Accelerated maritime cyber rules. NIS2 finalized in Europe with significantly expanded scope and penalties.

The regulatory environment transformed from encouraging security to mandating it.

What Each Framework Actually Requires

NIS2 (European Union)

Scope: Approximately 30,000 companies in Germany alone. Covers essential entities (energy, transport, health, water) and important entities (manufacturing, chemicals, food).

Penalties:

- Essential entities: €10 million or 2% of global turnover
- Important entities: €7 million or 1.4% of turnover
- **Personal liability:** Executives can face temporary bans from management roles

Key OT requirements:

- 24-hour early warning for significant incidents
- 72-hour full incident report
- Final report within one month
- Network segmentation between IT and OT
- Supply chain security assessments
- ICS network visibility controls

The personal liability provision is notable—this puts executive attention on OT security in a way voluntary frameworks never achieved.

TSA Security Directives (Pipeline & Rail)

Background: First issued May 27, 2021—weeks after Colonial Pipeline. Multiple updates through SD-02F.

Key requirements:

- Report cybersecurity incidents to CISA within 24 hours
- Designate Cybersecurity Coordinator available 24/7
- TSA-approved Cybersecurity Implementation Plan
- Test incident response plan annually (minimum two objectives)
- Assess 100% of security measures every three years
- IT/OT network segmentation

The 24-hour reporting requirement creates obligations many organizations weren't prepared to meet. Determining whether an incident rises to the reporting threshold requires situational awareness that detection tools alone can't provide.

MTSA Maritime Cybersecurity (US)

Timeline:

- July 16, 2025: Cyber incident reporting begins
- January 12, 2026: Cybersecurity training deadline
- July 16, 2027: Full Cybersecurity Plan requirements

Key requirements:

- Develop Cybersecurity Plan
- Appoint Cybersecurity Officer (CySO)
- Conduct penetration testing
- Network segmentation
- Alignment with NIST CSF and CISA CPGs

Organizations in the maritime sector should note the July 2025 reporting deadline is approaching rapidly.

NERC CIP (Electric Sector)

The most mature OT security regulatory framework continues evolving:

Recent updates:

- CIP-015-01 (INSM): Requires Internal Network Security Monitoring—approved June 2025
- CIP-002-8: Tightens Control Center definitions
- CIP-003: Updated security requirements (effective April 2026)
- Enhanced supply chain security controls

The INSM requirement is significant—it mandates monitoring within OT networks, not just at perimeter boundaries.

IEC 62443

Accepted as IEC "horizontal standards" in November 2021, meaning all sector-specific OT standards must use IEC 62443 as foundation.

- 45% adoption increase in 2024
- 50+ member companies in ISA Global Cybersecurity Alliance
- Four Security Levels (SL1-SL4) from unintentional misuse to nation-state attacks

IEC 62443 increasingly appears in procurement requirements. Vendors face pressure to demonstrate compliance; asset owners use it to establish security requirements.

Does Compliance Produce Security?

This is the central question for any regulatory framework.

The uncomfortable macro data:

- 59% increase in cybersecurity budgets year-over-year
- 61% of organizations still experienced breaches

Organizations are spending more without achieving proportionally better outcomes. This suggests that how money is spent matters more than how much—and that compliance spending doesn't always translate to security improvement.

But regulated sites perform measurably better:

> *"Regulated sites experienced approximately 50% fewer financial losses and safety impacts. They didn't have fewer incidents—they had better capabilities to contain and recover." — SANS 2025*

The mechanism matters here. Regulations that require incident response plans, testing, and assessment produce value not through preventing compromise but through forcing organizations to operationalize discipline. IR plans that must exist get practiced. Controls that must be documented get implemented.

The non-compliance premium:

Organizations with high regulatory non-compliance face $5.05 million in breach costs—a 12.6% premium over compliant organizations. The correlation between compliance and better outcomes is measurable.

The Compliance Theater Risk

Not all compliance activity produces security. Organizations can document policies without operationalizing them. Assessments can confirm theoretical controls without testing whether they function. Audit preparation can consume resources that might otherwise improve actual security posture.

Signs of compliance theater:

- Policies that exist on paper but aren't followed under operational pressure
- Audit evidence that reflects theoretical rather than actual practices
- Remediation plans that never complete before the next audit cycle
- Documentation consuming more resources than capability development

The gap between regulatory intent and operational implementation remains significant. Organizations that treat compliance as documentation exercise rather than capability development achieve neither security nor sustainable compliance.

The Path Forward

1. **Treat compliance as floor, not ceiling** — Regulatory requirements represent minimum expectations, not the definition of adequate security. Organizations that stop at compliance remain vulnerable.
2. **Operationalize, don't just document** — Practiced incident response plans outperform documented ones. Controls that are tested work better than controls that are assumed.
3. **Map across frameworks** — Organizations subject to multiple regulations can find common controls. Implement to the highest standard; document once for multiple requirements.
4. **Anticipate requirements** — Today's emerging risks become tomorrow's mandates. The pattern of post-incident regulation is predictable. Organizations that build capability ahead of requirements avoid compliance scrambles.
5. **Use frameworks for capability development** — NIST CSF, IEC 62443, and CISA CPGs provide structure for security programs beyond regulatory minimums. Organizations that adopt frameworks strategically build more sustainable programs.

Compliance tells you what you must do. Security outcomes tell you whether it's working.

Sources

- European Parliament, NIS2 Directive: https://eur-lex.europa.eu/eli/dir/2022/2555
- Transportation Security Administration, Security Directives: https://www.tsa.gov/sd-and-ea
- U.S. Coast Guard, MTSA Cybersecurity Requirements: https://www.federalregister.gov/documents/2025/01/17/2024-31230/cybersecurity-in-the-marine-transportation-system
- NERC, CIP Standards: https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
- SANS Institute, State of ICS/OT Security 2025: https://www.sans.org/white-papers/state-of-ics-ot-security-2025
- CISA, Cross-Sector Cybersecurity Performance Goals: https://www.cisa.gov/cross-sector-cybersecurity-performance-goals
- IEC 62443 Series: https://www.iec.ch/blog/understanding-iec-62443