Congressional Research Service
Informing the legislative debate since 1914

Cybersecurity: Considerations on Regulatory Harmonization

June 26, 2026

Congressional Research Service
https://crsreports.congress.gov
R49009

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R49009

June 26, 2026

Chris Jaikaran
Specialist in Cybersecurity Policy

Cybersecurity: Considerations on Regulatory Harmonization

The Department of Homeland Security (DHS) is simultaneously pursuing three major cybersecurity regulatory initiatives—each issued by a different agency, each addressing a different critical infrastructure sector, and each with its own definitions, timelines, and reporting requirements for cybersecurity incidents. Some stakeholders have raised concerns about the potential burdens that the three separate, but overlapping, mandates may impose on regulated entities. The three rules are:

- the U.S. Coast Guard's (USCG) Cybersecurity in the Marine Transportation System,
- the Transportation Security Administration's (TSA) proposed rule Enhancing Surface Cyber Risk Management, and
- the Cybersecurity and Infrastructure Security Agency's (CISA) proposed rule implementing the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).

All three would require cyber incident reporting. The USCG and TSA rules would also impose some cybersecurity standards on business operations.

The USCG rule became effective July 16, 2025, applying to U.S.-flagged vessels, Outer Continental Shelf facilities, and facilities subject to the Maritime Transportation Security Act of 2002 (MTSA). It requires incident reporting to the National Response Center (NRC) immediately upon a reportable event, with a phased schedule for training and cybersecurity plan submissions. TSA's notice of proposed rulemaking (NPRM), issued on November 7, 2024, has not been finalized, but would cover approximately 293 pipeline, freight rail, passenger rail, and bus operators designated as high-risk if finalized. CISA's CIRCIA rule was proposed on April 4, 2024, and has also not yet been finalized, but would cover an estimated 316,000 entities across all 16 critical infrastructure sectors if finalized.

Despite sharing the common goal of reducing cyber risk to critical infrastructure, the three rules have notable differences. They use different definitions of a reportable cyber incident. They require reports to be sent to different agencies—the USCG rule directs reports to the NRC, TSA and the CIRCIA rule requires reports directly to CISA. They also impose different reporting timelines: USCG requires notification "without delay," TSA proposes a 24-hour window, and CIRCIA mandates 72 hours for substantial incidents and 24 hours for ransomware payments. For certain operators, such as maritime pipeline facilities classified as critical infrastructure, this fragmentation could require simultaneous compliance with all three regimes, potentially creating an administrative burden and adding complexity to the response. Some have suggested that regulatory harmonization is necessary to relieve covered entities from duplicative efforts. While there is this potential overlap, it is unclear how many facilities would be subject to the overlapping requirements, or if a push towards harmonization would quash sector-specific reporting benefits.

Despite no clear account of the scope of the problem, various stakeholders have been working toward potential solutions. The Office of the National Cyber Director (ONCD), the Government Accountability Office (GAO), industry groups, and (to some extent) cybersecurity regulatory agencies have all raised concerns about the proliferation of inconsistent cybersecurity requirements. For instance, a July 2025 GAO report found that industry participants believe the federal government has not made progress in harmonizing cybersecurity regulations. Meanwhile, through executive order, the Trump Administration has directed agencies to reduce regulatory burdens. This action could delay the timing and ultimate scope of the CIRCIA and TSA final rules.

If Congress chooses to address disparate cyber incident notification and response frameworks (which could result if all three rules are finalized and given effect), it has several options. It could codify a harmonized incident reporting framework by statute, resolving definitional inconsistencies that agencies have been unable to reconcile on their own. It could empower ONCD with binding cross-agency authority over cybersecurity harmonization. Alternatively, Congress could wait for the CIRCIA and TSA rulemaking processes to conclude and evaluate whether the resulting rules achieve sufficient harmonization before intervening legislatively.

Contents

Tables

Contacts

Introduction

Cybersecurity threats to critical infrastructure have grown in frequency and severity. Nation-state actors and transnational criminal organizations (i.e., cybercriminals) have targeted pipelines, railways, ports, water systems, and other essential services with increasing sophistication. The 2021 DarkSide ransomware attack on Colonial Pipeline—which caused a week-long shutdown of 5,500 miles of petroleum pipelines serving the Eastern Seaboard—served as a galvanizing event that accelerated federal regulation across multiple agencies.[1]

Three agencies within the U.S. Department of Homeland Security (DHS)—each with overlapping jurisdiction over transportation and critical infrastructure—have since moved to establish mandatory cybersecurity requirements. The U.S. Coast Guard (USCG), operating under authority granted by the Maritime Transportation Security Act of 2002 (MTSA, 46 U.S.C. §§70102-70103), issued a final rule for furthering the cybersecurity of the marine transportation system.[2] The Transportation Security Administration (TSA), using an authority under the Aviation and Transportation Security Act (49 U.S.C. §114(l)), published a notice of proposed rulemaking (NPRM) for pipeline, rail, and bus operators.[3] The Cybersecurity and Infrastructure Security Agency (CISA), pursuant to the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA, 6 U.S.C. §§681-681g), also published a proposed rule that would cover all 16 critical infrastructure sectors.[4] As of the time of writing, the TSA and CISA rules have not yet been finalized.

These three rules provide illustrative examples of the challenge of cybersecurity regulatory harmonization, which has been drawing Congressional interest for several years. Industry stakeholders have argued that they are facing increased costs and compliance burdens around regulations imposed by numerous agencies, a concern that Congress has been hearing with increasing frequency.[5]

This report provides a comparative analysis of these three regulations. It examines the scope, structure, and key requirements of each rule; identifies areas of convergence and divergence; and discusses the implications for congressional oversight and areas for potential legislative action.

Overview of Rulemaking

The process by which federal agencies issue binding regulations—rulemaking—is governed primarily by the Administrative Procedure Act (APA).[6] Under the standard *notice-and-comment* rulemaking process, an agency must publish a proposed rule in the *Federal Register* and provide the public an opportunity to comment on the rule. After reading the comments and making

[1] For more information on the Colonial Pipeline cyberattack, see CRS Insight IN11667, *Colonial Pipeline: The DarkSide Strikes*, by Paul W. Parfomak and Chris Jaikaran.

[2] DHS U.S. Coast Guard, "Cybersecurity in the Marine Transportation System," 90 *Federal Register* 6298-6453, January 17, 2025. (Hereinafter "Cybersecurity in the Maritime Transportation System.")

[3] DHS Transportation Security Administration, "Enhancing Surface Cyber Risk Management," 89 *Federal Register* 88488-88592, November 7, 2024. (Hereinafter "Enhancing Surface Cyber Risk Management.")

[4] DHS Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements," 89 *Federal Register* 23644-23776, April 4, 2024. (Hereinafter, "CIRCIA.")

[5] Committee on Oversight and Government Reform, "Hearing Wrap Up: Duplicative and Inconsistent Regulations Are Harming Industry Cybersecurity Capabilities; Harmonization Is Needed," press release, July 25, 2024, https://oversight.house.gov/release/hearing-wrap-up-duplicative-and-inconsistent-regulations-are-harming-industry-cybersecurity-capabilities-harmonization-is-needed.

[6] 5 U.S.C. §553.

adjustments to the rule, the agency must publish a final rule in the *Federal Register* and have at least a 30-day delay before the final rule takes effect.[7]

Congress shapes agency rulemaking through statute. Congress may grant an agency broad rulemaking authority, direct it to issue a specific rule, or remain silent on enforcement and compliance mechanisms. In some cases, responsibilities for rulemaking, compliance, and enforcement authority may end up divided among different agencies. For cybersecurity, the result has been a fragmented architecture in which multiple agencies hold overlapping authorities without a single coordinating entity.

Background on the Rules

CISA, TSA, and the USCG are all components of DHS. Congress has granted each agency unique authority over their regulated entities and all have chosen to issue rules (or proposed rules) addressing cyber risk.

CISA's Proposed Rule

Congress enacted CIRCIA as part of the Consolidated Appropriations Act, 2022 (P.L. 117-103, Div. Y), directing CISA to promulgate regulations requiring covered entities to report covered cyber incidents within 72 hours and ransomware payments within 24 hours. CISA published its NPRM on April 4, 2024. The statutory deadline for a final rule was October 2025, but as of June 2026, CISA had not yet finalized the rule, and was scheduling additional public listening sessions.[8]

The proposed CIRCIA rule is sweeping in scope. It would apply to approximately 316,000 entities across all 16 critical infrastructure sectors identified in Presidential Policy Directive-21 (PPD-21). Potentially affected companies include those in the chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors, transportation systems, and water and wastewater systems sectors. Entities that exceed the Small Business Administration (SBA) size standard for their industry are automatically covered; smaller entities may still be covered if they meet sector-based criteria.

The rule would establish a two-tier reporting structure. "Covered cyber incidents"—defined as substantial incidents meeting certain impact thresholds—must be reported within 72 hours.[9] Ransomware payments and amounts must be reported within 24 hours. CISA has enforcement authority, including the ability to issue requests for information (RFI). If those go unanswered, the agency has authority to issue administrative subpoenas. Failure to comply with a subpoena may result in referral to the Attorney General, acquisition penalties, or suspension and debarment from federal contracting.

A central feature of the CIRCIA rule is its harmonization mechanism. Entities that already report cybersecurity incidents under a sector-specific regulatory regime—for instance, healthcare

[7] The APA contains several exceptions to these procedural requirements; see 5 U.S.C. §553. For more information on the rulemaking processes, see CRS In Focus IF10003, *An Overview of Federal Regulations and the Rulemaking Process*, by Maeve P. Carey.

[8] For further information on CIRCIA, see CRS Report R48025, *CIRCIA: Notice of Proposed Rule Making: In Brief*, by Chris Jaikaran.

[9] CIRCIA p. 23645.

entities reporting under the Health Insurance Portability and Accountability Act (HIPAA) or financial entities reporting to their regulators—may be exempt from CISA reporting if the existing reporting is deemed equivalent in content and timing, and a formal agreement exists between the sector regulator and CISA (to facilitate the sharing of information). This "substantially similar reporting exception" is intended to reduce duplicative burdens.[10]

USCG's Final Rule

The U.S. Coast Guard published its final rule, Cybersecurity in the Marine Transportation System, on January 17, 2025. The rule became effective July 16, 2025, and is codified at 33 C.F.R. Parts 101 and 160. It represents the first enforceable federal cybersecurity framework specifically designed for the maritime sector. Prior to the final rule, USCG had issued guidance to maritime operators to incorporate cybersecurity into their existing security plans.[11]

The rule applies to owners and operators of U.S.-flagged vessels, Outer Continental Shelf (OCS) facilities, and facilities already required to maintain security plans under MTSA—namely those regulated under 33 C.F.R. Parts 104, 105, and 106. It does not expand MTSA's jurisdictional reach to new categories of entities; instead, it adds cybersecurity obligations to those already within the MTSA framework.

Implementation is phased over a three-year period. As of July 16, 2025, all regulated entities must report "reportable cyber incidents" to the National Response Center (NRC) without delay.[12] By January 12, 2026, all personnel with access to information technology (IT) or operational technology (OT) systems must complete initial cybersecurity training. By July 16, 2027, owners and operators must designate a Cybersecurity Officer (CySO), conduct a Cybersecurity Assessment, and submit a Cybersecurity Plan to the USCG for approval.

The USCG separately sought public comment on whether a two-to-five-year additional delay should be granted for U.S.-flagged vessels, given comments from the maritime industry about implementation difficulties. As of this writing, no final decision on that delay has been published.

TSA's Proposed Rule

Prior to 2021, TSA issued cybersecurity *guidelines* for four surface transportation sector modes (i.e., mass transit, freight rail, highway motor carrier, and pipelines) which could be *voluntarily* adopted.[13] Given the voluntary nature of these guidelines, their adoption was not tracked by TSA. Further, the voluntary approach was criticized for being unenforceable and resulting in uneven application.[14]

---

[10] CIRCIA p. 23769.

[11] USCG, Reporting Breaches of Security, Suspicious Activity, Transportation Security Incidents, and Cyber Incidents," *Navigation and Vessel Inspection Circular No. 02-24*, February 1, 2024, https://www.dco.uscg.mil/Portals/9/OCSNCOE/References/NVICs/NVIC-02-24.pdf?ver=UeyeMurGGG3bbTvzyS-ojg%3d%3d, since superseded by Change 1 on November 12, 2025, https://www.uscg.mil/Portals/0/Images/cyber/BOS_SA_Cyber%20Reporting%20NVIC%2002-24%20CH%201.pdf?ver=T480tZ3n3fUUmnvNwRay5w%3d%3d.

[12] Cybersecurity in the Maritime Transportation System, p. 23650.

[13] Transportation Security Administration, TSA Cybersecurity Roadmap 2018, https://www.tsa.gov/sites/default/files/tsa_cybersecurity_roadmap.pdf.

[14] U.S. Department of Transportation, Office of Inspector General, May 21, 2008, p. 6. Provisions in the Pipeline Inspection, Protection, Enforcement, and Safety Act of 2006 (P.L. 109-468) required the Inspector General to "address the adequacy of security standards for gas and oil pipelines" (§23(b)(4)). For further information, see CRS Report R46903, *Pipeline Cybersecurity: Federal Programs*, by Paul W. Parfomak and Chris Jaikaran.

In the wake of the May 2021 ransomware attack against Colonial Pipeline,[15] and in an effort to prevent future attacks, TSA used its authority to issue mandatory security directives on an emergency basis (under 49 U.S.C. §114(l)). TSA issued two directives, requiring critical pipeline operators to establish a cybersecurity coordinator, report cybersecurity incidents, assess cyber vulnerability, and implement prescriptive measures and practices to defend against cyber threats. Since those original directives, TSA has issued more than twenty security directives related to cybersecurity for the pipeline and rail industries.[16] These directives require a variety of actions, including assigning responsibilities to specific company employees, planning, vulnerability assessments, and incident reporting.

On November 7, 2024, TSA released an NPRM related to pipeline, rail, and bus cyber risk management.[17] This NPRM is the follow-on to a 2022 advanced notice of proposed rulemaking (ANPRM).[18] The proposed rule would mandate that rail and pipeline companies:

- have a TSA-approved cyber risk management program which would include evaluations, plans, and prescribed security outcomes (with the exception of over-the-road bus operators);
- report cyber incidents to CISA; and
- account for physical security concerns.[19]

The comment period for the NPRM was open until February 5, 2025.[20] Once implemented, the final rule will create a mandatory standard for cybersecurity operations at the covered entities. TSA expects this rule to reduce cybersecurity risks by:

- driving adoption of practices that reduce the ability for threat actors to exploit networks (e.g., patch management and network segmentation);
- reducing the time to recovery post incident by ensuring backups of systems are available;
- maintaining constant visibility of systems through continuous monitoring; and
- improving operations through planning and exercising.[21]

The proposed rule would cover approximately 293 entities: 73 freight railroads, 34 public transportation agencies and passenger railroads, 71 over-the-road bus (OTRB) operators, and 115 pipeline facilities and systems. These entities were selected based on risk-tiered criteria. A full Cyber Risk Management (CRM) program is required for higher-risk freight rail, passenger rail, and pipeline operators; OTRB operators face the more limited requirement of reporting cybersecurity incidents to CISA.

TSA's CRM program has three primary components: (1) an annual enterprise-wide cybersecurity evaluation comparing the entity's current security posture to a target profile aligned with the NIST Cybersecurity Framework (CSF); (2) a Cybersecurity Operational Implementation Plan

[15] CRS Insight IN11667, *Colonial Pipeline: The DarkSide Strikes*, by Paul W. Parfomak and Chris Jaikaran.

[16] "Security Directives and Emergency Amendments," Transportation Security Administration, https://www.tsa.gov/sd-and-ea.

[17] Enhancing Surface Cyber Risk Management.

[18] Enhancing Surface Cyber Risk Management.

[19] "TSA Announces Proposed Rule That Would Require the Establishment of Pipeline and Railroad Cyber Risk Management Programs," Transportation Security Administration, https://www.tsa.gov/news/press/releases/2024/11/06/tsa-announces-proposed-rule-would-require-establishment-pipeline-and.

[20] Enhancing Surface Cyber Risk Management.

[21] Enhancing Surface Cyber Risk Management.

(COIP) that designates responsible personnel and prescribes measures to identify, protect, detect, respond to, and recover from cyber incidents; and (3) a Cybersecurity Assessment Plan (CAP) establishing schedules and annual reports for assessments.

As of June 2026, TSA had not yet finalized the rule.

Comparison of the Rules

The three rules share some important components. **Table 1** provides an overview of each rule across common elements.

Table 1. Comparison of the DHS Cybersecurity Rules

Element	CISA (CIRCIA Rule)	TSA (Surface Cyber Rule)	USCG (MTS Rule)
Status	Proposed rule (NPRM, April 4, 2024); not yet finalized	Proposed rule (NPRM, Nov. 7, 2024); not yet finalized	Final rule (effective July 16, 2025, phased implementation through July 2027)
Issuing Agency	Cybersecurity and Infrastructure Security Agency (CISA), DHS	Transportation Security Administration (TSA), DHS	U.S. Coast Guard (USCG), DHS
Legal Authority	Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), P.L. 117-103	49 U.S.C. §114(l); Implementing Recommendations of the 9/11 Commission Act of 2007	Maritime Transportation Security Act of 2002 (MTSA), 46 U.S.C. §70103, as amended 2018
Sectors Covered	All 16 critical infrastructure sectors (i.e., chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare, IT, nuclear, transportation, water/wastewater)	Surface transportation: freight railroads, passenger railroads, rail transit, pipeline facilities/systems, and over-the-road bus (OTRB) operators	Marine Transportation System: U.S.-flagged vessels, Outer Continental Shelf (OCS) facilities, and MTSA-regulated facilities (ports, waterfront facilities)
Estimated Covered Entities	~316,000 entities across all sectors	~293 designated owner/operators (73 freight rail, 34 passenger rail/transit, 71 OTRB, 115 pipeline)	All MTSA-regulated entities (vessels with Vessel Security Plans, facilities with Facility Security Plans)
Covered Entity Threshold	Entities in a critical infrastructure sector exceeding SBA small-business size standard, or meeting sector-based criteria regardless of size	Risk-tiered criteria set by TSA; higher-risk operators required to have full CRM program; OTRB operators limited to incident reporting only	Entities already subject to MTSA security plan requirements (33 C.F.R. Parts 104, 105, 106); no expansion of MTSA jurisdiction
Incident Reporting: To Whom	CISA (directly via CISA reporting portal)	CISA (for cybersecurity incidents); TSA (for	USCG National Response Center (NRC); also CISA and FBI under pre-existing

Element	CISA (CIRCIA Rule)	TSA (Surface Cyber Rule)	USCG (MTS Rule)
		physical security concerns)	33 C.F.R. §6.16-1 for some entities
Incident Reporting: Timeline	72 hours for covered cyber incidents and 24 hours for ransomware payments	24 hours after identification of a reportable cybersecurity incident (for pipeline, rail, and higher-risk bus)	"Without delay" for reportable cyber incidents
Definition of Reportable Incident	*Covered cyber incident*: substantial loss of confidentiality, integrity, or availability; disruption to critical functions; unauthorized access to OT/ICS; or impact on national security, economic security, or public health/safety	*Reportable security incident*: incidents impacting or likely to impact operational systems; aligns with CISA definitions for purposes of incident reporting	*Reportable cyber incident*: substantial loss of CIA of covered IT/OT; disruption to business operations with public health/safety risk; unauthorized disclosure of nonpublic personal information; potential operational disruption to critical infrastructure assets; or incidents that may lead to a TSI
Cybersecurity Plan / Program Required	No standalone cybersecurity plan required; reporting obligations only (incident reports and supplemental reports)	TSA-approved Cyber Risk Management (CRM) Program required, including: annual cybersecurity evaluation, Cybersecurity Operational Implementation Plan, and Cybersecurity Assessment Plan	Cybersecurity Plan required, submitted to USCG for approval; must address account security, device protection, data safeguarding, network segmentation, supply chain risk, penetration testing, resilience, and reporting protocols
Cyber Incident Response Plan	Not specifically required under CIRCIA rule; separate from reporting obligations	Required for all covered owner/operators regardless of whether Critical Cyber Systems are identified	Cyber Incident Response Plan required as part of the broader Cybersecurity Plan; must identify roles, responsibilities, and decision authorities
Designated Cybersecurity Officer (or similar)	Not required under CIRCIA rule	Cybersecurity Coordinator required; accountable executive must be designated in plans	Cybersecurity Officer required to be designated by July 16, 2027; responsible for assessment, plan development, and incident response oversight
Training Requirements	Not specified in CIRCIA rule	Security training for security-sensitive employees required for OTRB operators using TSA-approved curriculum	Annual cybersecurity training required for ALL personnel with IT/OT access; initial deadline January 12, 2026; new hires must complete training within 30 days of hiring

Element	CISA (CIRCIA Rule)	TSA (Surface Cyber Rule)	USCG (MTS Rule)
Assessment / Audit Requirements	Not required; CISA may request information or issue subpoenas	Annual enterprise-wide cybersecurity evaluation; Cybersecurity Assessment Plan with annual report; third-party assessors must be independent	Cybersecurity Assessment required before plan submission; USCG retains authority to conduct inspections and audits to verify plan implementation
Enforcement Mechanism	Administrative subpoena; referral to Attorney General; acquisition penalties; suspension/debarment from federal contracting; criminal penalties for false statements	TSA enforcement authority under 49 U.S.C. §114; civil penalties; denial of plan approval	MTSA penalty framework; corrective action orders; civil and criminal penalties; increased unannounced inspections; suspension/revocation of security plan approval; denial of port entry
Waivers / Exemptions	Small business exemption (SBA size standard) unless entity meets sector-based criteria; substantially similar reporting exception for entities reporting to other regulators	Applicability determined by TSA risk-tiering; some requirements inapplicable to lower-risk entities	Waivers available if cybersecurity requirements are unnecessary given operating conditions; equivalence determinations available for international standard compliance
Harmonization with Other Rules	Substantially similar reporting exception allows exemption from CISA reporting if sector regulator has equivalent regime and formal agreement with CISA; CISA directed to consult Cyber Incident Reporting Council	TSA explicitly solicited comments on regulatory harmonization opportunities; rule aligns with NIST CSF 2.0 and CISA CPGs; incident reporting directed to CISA	Declined to adopt CIRCIA's definition of *substantial cyber incident*; reporting directed to NRC rather than CISA; USCG stated complementary but distinct operational purposes
Framework / Standards Reference	No specific framework prescribed; CIRCIA defines covered incidents by impact	NIST Cybersecurity Framework (CSF) 2.0; CISA Cross-Sector Cybersecurity Performance Goals (CPGs)	International Maritime Organization (IMO) Resolution MSC.428(98); alignment with NIST CSF encouraged but not mandated
Implementation Timeline	Final rule not yet published.	Final rule not yet published.	Phased: Incident reporting (July 16, 2025); Training (January 12, 2026); CySO designation and Plan submission (July 16, 2027)
Estimated Compliance Cost	Estimated $1.4 billion to industry over an 11-year period.	Estimated $2.14 billion over 10 years across all covered modes	Estimated to increase compliance costs $1.2 billion beyond previous requirements (the time period is undisclosed)

Source: CRS analysis of CIRCIA, Cybersecurity in the Maritime Transportation System, and Enhancing Surface Cyber Risk Management.

Notes: Department of Homeland Security (DHS). Cybersecurity and Infrastructure Security Agency (CISA). Transportation Security Administration (TSA). U.S. Coast Guard (USGC). Over the Road Bus (ORTB). Outer Continental Shelf (OCS). Small Business Administration (SBA). Cyber Risk Management (CRM). Information Technology (IT). Operational Technology (OT).

Areas of Convergence

All three rules are premised on the same foundational concern: that mandatory standards are necessary to address the evolving threat landscape. All three are anchored, at least in part, to the National Institute of Standards and Technology (NIST) Cybersecurity Framework, which provides a common vocabulary for identifying, protecting, detecting, responding to, and recovering from cyber incidents.[22] And all three recognize the critical distinction between information technology (IT) systems and operational technology (OT) systems (e.g., the control systems that govern cyber-physical processes such as pipeline flows, train operations, and port machinery).

CISA is the ultimate intended recipient of much of this reporting, either directly (under CIRCIA and TSA's proposed rule) or through existing mechanisms under 33 C.F.R. § 6.16-1 (for USCG-regulated entities that trigger the existing reporting requirement).

All three rules also require some form of incident reporting to the federal government. While the reporting destinations and timelines differ, the underlying goal is the same: to create a flow of timely, actionable threat intelligence that can be aggregated, analyzed, and shared to benefit the broader critical infrastructure community.

Areas of Divergence

Several differences between the three rules that may affect regulated entities should be noted, especially those in the following four areas: the reporting timelines, the type of incidents that must be reported, definitions, and positive cybersecurity controls.

First, the reporting timelines vary. CIRCIA mandates a 72-hour window for substantial incidents. TSA proposes a tighter 24-hour window, which is more aligned with its existing security directive framework. The USCG requires reporting "without delay," a phrase that the regulation does not define with a specific hour-based requirement. This will likely create compliance challenges for certain companies and may lead to operational confusion. For example, a maritime pipeline facility could fall under all three regimes, and be uncertain as to whether it needs to report an incident to three different agencies on three different timelines.

Second, the definitions of a reportable incident differ materially. The USCG rule created a new defined term—*reportable cyber incident*—that differs from CIRCIA's proposed definition of a *covered cyber incident*, despite acknowledging CIRCIA in the rulemaking. Commentators have noted that this creates "inconsistent reporting requirements for maritime critical infrastructure with respect to (1) which agencies must be notified, (2) when the agencies must be notified, and (3) the criteria under which the notification needs to be made."[23] A maritime transportation entity subject to all three rules may face different threshold questions depending on which regulation it is trying to satisfy.

[22] NIST, "The NIST Cybersecurity Framework (CSF) 2.0," February 26, 2024, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

[23] Erik Dullea et al., "The Coast Guard's Maritime Cybersecurity Rule Takes Effect," *Byte Back*, July 31, 2025, https://www.bytebacklaw.com/2025/07/the-coast-guards-maritime-cybersecurity-rule-takes-effect/.

Third, the reporting destinations differ. The USCG rule directs reports to the National Response Center. TSA's and CISA's proposed rules would direct reports to CISA. The USCG stated in the final rule that its reporting requirements serve "complementary but distinct operational purposes" to CISA reporting.[24]

Fourth, the sophistication of required cybersecurity programs differs significantly across rules. CISA's CIRCIA rule is a reporting rule: it does not require a cybersecurity plan, a cybersecurity officer, training, or any specific controls. TSA's proposed rule would require a comprehensive CRM program with TSA approval. The USCG rule requires the most comprehensive set of obligations: incident reporting, training, a designated officer, a cybersecurity assessment, and a formal cybersecurity plan subject to agency review. For entities that fall under multiple rules, the result is a layered but inconsistent compliance framework.

The Harmonization Challenge

> **"**There are always trade-offs. This is one of the rare cases where the tradeoff is entirely within the government. The trade-off here is a coordination problem inside the government.**"**
>
> *- Nick Leiserson, former Assistant National Cyber Director for Cyber Policy and Programs, CyberNext DC 2024, December 12, 2024*

A core purpose of cyber incident reporting is to aggregate intelligence about active threats, identify patterns, and share that intelligence back to defenders quickly. That purpose may be undermined when incidents are reported to different agencies on different timelines under different thresholds, because no single agency develops a complete picture of the entire threat landscape. At the same time, varied characteristics across the array of all businesses and other regulated entities—including their industry, resources, and cyber risk profile—creates opportunities for tailoring different aspects of regulation to different circumstances. Finding the appropriate balance between these objectives creates regulatory challenges.

The Office of the National Cyber Director (ONCD, a congressionally authorized entity within the Executive Office of the President that advises the President on matters related to cybersecurity) identified regulatory harmonization as a top priority in 2023.[25] ONCD issued a request for information (RFI) that received 86 responses from 11 of the 16 critical infrastructure sectors.[26] The ONCD's summary of its RFI found overwhelming consensus that "a lack of cybersecurity regulatory harmonization and reciprocity posed a challenge to both cybersecurity outcomes and business competitiveness."[27] Former National Cyber Director Harry Coker noted that the trend line was "generally heading toward more fragmentation, not more harmonization."[28]

GAO's solicited industry perspectives on cyber regulatory harmonization that reinforced the ONCD's assessment. Industry participants in panel discussions stated that the federal government

[24] Cybersecurity in the Maritime Transportation System, p. 6321.

[25] Office of the National Cyber Director, "Request for Information on Cyber Regulatory Harmonization; Request for Information: Opportunities for and Obstacles to Harmonizing Cybersecurity Regulations," 88 *Federal Register* 55694-55697, August 16, 2023.

[26] Harry Coker, Jr., "We Need to Harmonize Cybersecurity Regulations, What We Heard from Our Partners," blog post, June 4, 2024, https://bidenwhitehouse.archives.gov/oncd/briefing-room/2024/06/04/we-need-to-harmonize-cybersecurity-regulations-what-we-heard-from-our-partners/. (Hereafter "ONCD Blog.")

[27] ONCD Blog.

[28] ONCD Blog.

has made "limited progress" on harmonization.[29] One participant summarized the situation bluntly: "We are no closer today than we were 10 years ago on creating a solution for harmonization."[30] The same report documented that some industry participants spend up to 50 percent of their staff's time on cybersecurity regulatory compliance—time diverted from actually securing systems.[31]

As of May 2026, both the TSA and CISA NPRMs have not yet been finalized. As noted previously, the Trump Administration introduced Executive Order 14192 which directed agencies to identify regulations for elimination or reduction.[32] It is unclear whether the implementation of this order may have an effect on TSA's and CISA's ability to finalize their proposed rules. The Trump Administration's March 2026 national cybersecurity strategy emphasized a goal to "promote common-sense regulation" and alignment of CIRCIA "with industry preferences to reduce regulatory burden."[33]

Considerations for Congress

These three abovementioned rules were released by entities within the same department (DHS), yet they contain elements that could contribute to operational uncertainty for covered entities. A growing area of concern among industry regarding cybersecurity regulation is the lack of harmonization among regulators.

Congress has several options as it oversees the development and implementation of federal cybersecurity regulations. The considerations below represent distinct but not mutually exclusive options. Each carries trade-offs between security outcomes, regulatory burden, agency autonomy, and legislative feasibility.

Mandate Common Definitions and Reporting Standards

The most significant source of divergence across the three rules is the inconsistency in cyber incident reporting definitions, timelines, and reporting destinations. Within DHS, the Secretary could direct the components to resolve this in their rulemaking. This approach would likely require the USCG to align its "reportable cyber incident" standard and its NRC reporting requirement with the proposed CIRCIA framework.

Across all regulators, Congress may choose to resolve the potential for regulatory inconsistencies through legislation that establishes a single, statutory definition of a "reportable cybersecurity incident" applicable across all federal agencies, sets a uniform reporting timeline (e.g., 72 hours) for covered incidents, and designates a single agency as the primary and sole recipient of all critical infrastructure cyber incident reports. For instance, Congress could require all agencies to enter into information-sharing agreements with a potentially designated primary agency, directing reports onward to sector risk management agencies (SRMA) and regulators. While such legislation would constrain agency discretion, it would provide greater clarity for the regulated

[29] U.S. Government Accountability Office, *Cybersecurity Regulations: Industry Perspectives on the Impact, Progress, Challenges, and Opportunities of Harmonization*, GAO-25-108436, July 30, 2025, https://www.gao.gov/assets/gao-25-108436.pdf. (Hereinafter, "GAO-25-108436.")

[30] GAO-25-108436, p. 6.

[31] GAO-25-108436, p. 5.

[32] E.O. 14192.

[33] The White House, "President Trump's Cyber Strategy for America," March 2026, https://www.whitehouse.gov/wp-content/uploads/2026/03/President-Trumps-Cyber-Strategy-for-America.pdf; for more information, see CRS Insight IN12667, *The Trump Administration's Cyber Strategy*, by Chris Jaikaran.

community and improve the federal government's ability to aggregate and act on threat intelligence. Should Congress choose to pursue establishing more specific direction for agencies, implications of *Loper Bright Enterprises v. Raimondo* may require lawmakers to draft specific statutes and express authorities for agencies.[34]

If agencies continue to use different definitions of *cyber incident*, *substantial impact*, or *critical system*, entities operating across sectors—such as energy companies, which may be subject to existing federal cyber regulations (e.g., Federal Energy Regulatory Commission) and CIRCIA, or pipeline operators subject to both TSA and CISA requirements—will likely continue to face confusion regardless of which reporting infrastructure is in place. Respondents to GAO's discussions supported using NIST CSF as a definitional baseline, reflecting the fact that a consensus framework already exists. Congress would not need to invent new terminology where it did not wish to, and instead mandate adoption of the NIST CSF in whole or in part.[35] Standardized definitions could also be phased in and Congress could consider waiving various aspects of the rulemaking process to expedite the changes.

Alternatively, Congress may consider leaving agency variation on cybersecurity reporting requirements and definitions in place. Sector-specific regulators may argue that their particular definitions are calibrated to the risk profiles of the entities they oversee: a maritime cybersecurity incident involving vessel navigation systems has different characteristics than a financial market cyber event, and a single definition may be either too broad or too narrow for any given sector. The SEC, for example, operates under its own statutory mandates for securities disclosure that may not map cleanly onto CIRCIA-derived definitions of a cyber incident. As cyber threats evolve rapidly, any definition codified in statute may lag behind the threat environment.

A concern raised for consolidated reporting is around the security of the information. Industry groups have raised the prospect that consolidating sensitive cybersecurity information about companies at a single agency may raise their cybersecurity risk exposure in ways that are not offset by the increased understanding of national cybersecurity risk by agencies having that information.[36] Their concern is that an adversary could compromise the portal used to submit cyber incident reports, or the datastore itself, gaining access to sensitive information. Federal agencies have a history of collecting sensitive corporate information, however, and it is uncertain the extent to which agencies would be unable to secure that information. Further, a firm's cyber risk neither increases nor decreases with a report, as the risk exists regardless of the firm's cataloguing and conveying it.

Empower a Single Harmonization Authority

The DHS rules discussed in this report highlight the challenges of developing rules within different agencies operating under different statutory frameworks. Furthermore, the challenges compound when factoring in all federal cybersecurity regulations across the entire federal enterprise.

The Streamlining Federal Cybersecurity Regulations Act (S. 1875), introduced in May 2025 would establish an interagency Harmonization Committee led by the National Cyber Director.

[34] For further information on the Loper Bright decision, see CRS Report R48320, *Loper Bright Enterprises v. Raimondo and the Future of Agency Interpretations of Law*, by Benjamin M. Barczewski.

[35] GAO-25-108436.

[36] Jeff Gunnulfsen, "Enhancing Surface Cyber Risk Management Notice of Proposed Rulemaking, 89 *Federal Register* 88488 (Nov. 7, 2024), Docket No. TSA-2022-0001," comments by the American Fuel and Petrochemical Manufacturers, February 5, 2025, https://afpm.org/sites/default/files/issue_resources/TSA%20SD%20NPRM%20CommentsFINAL2-5-2025.pdf.

The committee would develop baseline and sector-specific cybersecurity requirements, issue advisory reports to agencies developing new rules, conduct a pilot program with three to five participating agencies, and report annually to Congress. The bill would also give ONCD a formal coordinating role it currently lacks. As a former ONCD official testified, having a "clear mandate from Congress to bring everyone to the table" would allow ONCD to lead the kind of cross-agency harmonization effort that individual agencies lack incentives to undertake on their own.[37] Congress could consider strengthening the bill further by requiring agency compliance with ONCD harmonization guidance, rather than treating it as advisory.

Proponents of the bill argue that its approach builds on an existing institutional infrastructure—ONCD was created by Congress in the FY2021 National Defense Authorization Act (P.L. 116-283), and serves as the principal cybersecurity policy coordinator within the Executive Office of the President.[38] The bill limits the Harmonization Committee to consultation on new rules and a voluntary pilot program.[39] ONCD's leadership testified before the Senate Homeland Security and Governmental Affairs Committee (HSGAC) that such legislation would "allow ONCD to better carry out our mission by bringing independent regulatory commissions to the table in a policymaking process" more quickly than existing administrative mechanisms.[40]

The bill's voluntary pilot program structure may be intended to preserve a degree of individual agency discretion, but may limit its impact on improving harmonization. As currently envisioned, participation by both agencies and regulated entities in the program would be voluntary. If a large enough contingent of either group opts not to participate, then there may be limits on how well the harmonization framework actually functions. Moreover, under the framework established under the Streamlining Federal Cybersecurity Regulations Act, an agency could consult with the committee and proceed with a regulation that diverges from the baseline framework, leaving fragmentation intact. The bill also does not directly address the noncongruence of pre-existing regulations and would only apply to new regulations.

Direct Reciprocity Among Sector Regulators

Distinct from harmonization, which seeks consistency in requirements, reciprocity refers to agencies accepting each other's compliance assessments. For example, if a maritime pipeline operator has completed a USCG-approved cybersecurity plan and passed an audit, under a reciprocity arrangement it would not be required to undergo a separate similar assessment or requirement by another agency. The DHS Secretary could direct CISA, TSA, and USCG to develop formal reciprocity agreements recognizing each other's compliance determinations for the same or overlapping entities. Congress may also do this through legislation that applies to all federal regulators. This approach would not require uniform requirements across all sectors (which may be inappropriate given sector-specific risks) but would reduce compliance burdens for multi-modal entities. The CIRCIA proposed rule's "substantially similar reporting exception"

[37] U.S. Congress, Senate Homeland Security and Governmental Affairs Committee, *Streamlining the Federal Cybersecurity Regulatory Process: The Path to Harmonization*, 118th Cong., 2nd sess., June 5, 2024, S.Hrg. 118-353 (Washington: GPO, 2024), https://www.congress.gov/118/chrg/CHRG-118shrg56046/CHRG-118shrg56046.pdf.

[38] 6 U.S.C. §1500.

[39] Megan L. Brown et al., "Call for Cybersecurity Regulatory Harmonization Ramp Up in Congress, White House," alert, June 7, 2024, https://www.wiley.law/alert-Calls-for-Cybersecurity-Regulatory-Harmonization-Ramp-Up-in-Congress-White-House.

[40] U.S. Congress, Senate Homeland Security and Governmental Affairs Committee, *Streamlining the Federal Cybersecurity Regulatory Process: The Path to Harmonization*, 118th Cong., 2nd sess., June 5, 2024, S.Hrg. 118-353 (Washington: GPO, 2024), p. 4, https://www.congress.gov/118/chrg/CHRG-118shrg56046/CHRG-118shrg56046.pdf.

represents a partial step in this direction, but it would require a formal agency-to-agency agreement that has not yet been established for all relevant sector pairs.[41]

This option would work within existing statutory authority without requiring broad legislative restructuring. By directing CISA to negotiate and finalize interagency agreements, Congress could reduce duplicative reporting obligations for the most heavily regulated entities without reorganizing agency jurisdictions or creating new administrative bodies. For entities such as pipeline operators simultaneously subject to TSA security directives and the forthcoming CIRCIA final rule, a robust substantially similar agreement between TSA and CISA could mean a single report would satisfy both reporting requirements. A standardized intake portal, already partly operational through existing CISA infrastructure, could be expanded to serve as the universal submission mechanism, further reducing administrative friction (e.g., reformatting identical information for different agencies.)

The substantially similar exception has a significant limitation: CISA's 2024 NPRM was criticized by lawmakers and industry partners for setting the threshold for what constitutes *substantially similar information* so high that few if any existing agency reporting requirements would qualify. Representative Andrew Garbarino specifically urged CISA to "provide greater flexibility for making CIRCIA's 'substantially similar' exception available to covered entities."[42] Congress could specify the standard in statute to avoid the possibility that a future final rule could again define the exception so narrowly as to limit its impact. There is also a temporal concern: if CISA is to negotiate bilateral information-sharing agreements with all relevant regulatory agencies, the time-consuming process could leave the compliance burden largely unchanged for years after any legislation is enacted.

Establish Unified Reporting Infrastructure

For the DHS rules, the Secretary could direct updates to the regulations and establish a common reporting structure. Such unification would be more involved for other federal agencies' rules, however.

A number of industry participants and GAO reports have called for a single federal reporting portal through which covered entities could submit a single cyber incident report that would then be routed to relevant agencies.[43] Congress could direct the development of such a portal (potentially through CISA's existing reporting infrastructure), and require all federal agencies to accept reports submitted through it. This would address the practical burden of entities having to report simultaneously to NRC, CISA, and potentially other regulators. It would also improve data quality, since a fragmented reporting system generates fragmented data. Building a unified portal would require agency coordination, interoperability standards, and data-sharing agreements.

Yet, agencies engage in rulemaking because they are seeking to address a sector-specific need. Consolidation raises concerns about the loss of sector-specific expertise and informational needs. For example, the USCG's maritime rule was designed to align with the International Maritime Organization's cybersecurity frameworks, reflecting the global regulatory environment in which international shipping companies operate. Collapsing distinct domains into a single regulator risks producing rules that are inadequate for particular sectors, broadly. Further, if the designated lead

[41] CIRCIA, p. 23708.

[42] Letter from Andrew Garbarino, Representative, NY-2, to The Honorable Jen Easterly, Director, CISA, July 3, 2024, https://downloads.regulations.gov/CISA-2022-0010-0464/attachment_1.pdf.

[43] Weslan Hansen, "GAO, Industry Call for Unified Cyber Rules Across Critical Sectors," *MeriTalk*, August, 5, 2025, https://www.meritalk.com/articles/gao-industry-call-for-unified-cyber-rules-across-critical-sectors/.

agency itself faces resource constraints, as CISA has experienced in 2025 and 2026, the consolidation of oversight responsibility without commensurate resources could produce a worse outcome than the current fragmentation. Finally, authority consolidation would likely involve the realignment of authorities for agencies, which would implicate multiple congressional committees.

Evaluate the CIRCIA Rule's Scope Before Finalization

With CISA's final CIRCIA rule not yet finalized and CISA conducting additional stakeholder listening sessions through 2026, Congress has an opportunity to provide direction on the scope of the rule before it is finalized. The 2024 NPRM proposed to cover approximately 316,000 entities—a scope that attracted criticism from multiple stakeholder groups for being overly broad and administratively burdensome.[44] Congress could use oversight hearings, letters of direction, or appropriations language to signal that the final CIRCIA rule should prioritize clarity, workability, and alignment with other existing sector-specific regimes over breadth of coverage.

Address Multi-Modal Entities

The most complex compliance challenges fall on entities that operate across multiple transportation modes or that fall under multiple sector regulatory environments. A maritime terminal that handles both vessel traffic and pipeline operations may be subject to the USCG rule as an MTSA facility, the TSA proposed rule as a pipeline operator, and the CISA proposed rule as a critical infrastructure owner. Congress could direct USCG, TSA, and CISA to jointly develop a compliance guide or a unified assessment process for such multi-modal entities, ensuring that compliance with one agency's cybersecurity program is recognized as satisfying parallel requirements under another. Multi-modal entities have previously shown a willingness for regulations and to engage with the government on creating those regulations, but have warned against the compounding burden on their operators.[45]

Concluding Thoughts

The current Administration's deregulatory posture under Executive Order 14192 could create a specific concern that cybersecurity rules may be weakened or delayed beyond Congress's intent with regards to national security. TSA's proposed surface cyber rule and the CISA proposed rule are both under development in an environment where agencies are under pressure to reduce regulatory burdens. Congress may wish to establish, through legislation or oversight, that cybersecurity requirements for critical infrastructure are a national security imperative that may not be subject to the same considerations and processes (e.g., a cost-benefit analysis) as other regulations.

[44] Michael T. Borgia, "CISA Delays Cyber Incident Reporting Rules Until May 2026," *Davis, Wright, Tremaine, LLP*, September 17, 2025, https://www.dwt.com/blogs/privacy—security-law-blog/2025/09/cisa-delays-cyber-incident-reporting-rules-2026.

[45] Kimberly Denbow, Vice President, Security and Operations, American Gas Association, "Testimony before the House Homeland Security Committee, Subcommittee on Transportation and Maritime Security, 'Impacts of Emergency Authority Cybersecurity Regulations on the Transportation Sector,'" November 19, 2024, https://www.aga.org/wp-content/uploads/2024/11/Denbow-Testimony-Cyber-NPRM-Hearing-Subcommittee-on-Transportation-and-Maritime-Security-Nov-19-2024.pdf.

Congress has considered the importance of agency cybersecurity rules relative to the evolving cybersecurity risk and involvement of the private sector, and may choose to continue doing so.[46] Congress has examined whether agencies are too slow in responding to cyber threats; have created a compliance burden for the private sector without a corresponding benefit (such as incident reports that are analyzed to create publicly releasable products on threats and mitigations); and whether or not there is a sufficiently strong private sector enterprise for cybersecurity that sufficiently addresses risk.[47] The benefit of improved cybersecurity reporting could help policymakers understand the cyber threat environment and help both public and private sector entities prioritize investments to address the greatest cybersecurity risks. The continued expansion of regulations may drive Congress to reconsider the scope, scale, and number of these regulations.

Author Information

Chris Jaikaran
Specialist in Cybersecurity Policy

Disclaimer

[46] U.S. Congress, House Homeland Security Committee, Cybersecurity and Infrastructure Protection Subcommittee, *Regulatory Harm or Harmonization? Examining the Opportunity to Improve the Cyber Regulatory Regime*, 119th Cong., 1st sess., March 11, 2025, Serial No. 119–7 (Washington: GPO, 2025).

[47] U.S. Congress, Senate Homeland Security and Governmental Affairs Committee, *Cyber Incident Reporting Act of 2021*, Report to Accompany S. 2875, 117th Cong., 2nd sess., December 13, 2022, S.Rept. 117-249 (Washington: GPO, 2023).