[9110-05-P]

DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

[Docket No. TSA-2022-0001]

RIN 1652-AA74

49 CFR Parts 1500, 1503, 1520, 1570, 1580, 1582, 1584, and 1586

Enhancing Surface Cyber Risk Management

AGENCY: Transportation Security Administration, DHS**.**

ACTION: Notice of proposed rulemaking (NPRM).

SUMMARY: The Transportation Security Administration (TSA) is proposing to impose cyber risk management (CRM) requirements on certain pipeline and rail owner/operators and a more limited requirement, on certain over-the-road bus (OTRB) owner/operators, to report cybersecurity incidents. With the proposed addition of requirements applicable to pipeline facilities and systems, TSA is also proposing that a requirement to have a Physical Security Coordinator and report significant physical security concerns be extended to the same facilities and systems. Finally, TSA is proposing clarifications and reorganization of other regulatory requirements necessitated by these changes.

DATES: Submit comments by **[INSERT DATE 90 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]**.

ADDRESSES:

Comments on this NPRM: You may submit comments on this NPRM, identified by the TSA docket number to this rulemaking, to the Federal Docket Management System (FDMS), a government-wide, electronic docket management system. To avoid duplication, please use only one of the following methods:

- *Electronic Federal eRulemaking Portal*: https://www.regulations.gov. Follow the online instructions for submitting comments.

- *Mail*: Docket Management Facility (M-30), U.S. Department of Transportation, 1200 New Jersey Avenue SE, West Building Ground Floor, Room W12-140, Washington, DC 20590-0001. The Department of Transportation (DOT), which maintains and processes TSA's official regulatory dockets, will scan the submission and post it to FDMS.
- *Fax*: (202) 493-2251.

See the **SUPPLEMENTARY INFORMATION** section for format and other information about comment submissions on the NPRM.

FOR FURTHER INFORMATION CONTACT:

General Questions: Ashlee Marks, Surface Division, Policy, Plans, and Engagement, TSA-28, Transportation Security Administration, 6595 Springfield Center Drive, Springfield, VA 20598-6028; telephone (571) 227-1039; email: *SurfaceCyberPolicy@tsa.dhs.gov.*

Legal Questions: Traci Klemm, Regulations and Security Standards, Office of Chief Counsel, Transportation Security Administration, 6595 Springfield Center Drive, Springfield, VA 20598-6002; telephone (571) 227-3583, or e-mail to *SurfaceCyberPolicy@tsa.dhs.gov.*

SUPPLEMENTARY INFORMATION:

Public Participation

TSA invites interested persons to participate in this NPRM by submitting written comments, including relevant data. We also invite comments relating to the economic, environmental, energy, or federalism impacts that might result from this rulemaking action. *See* the **ADDRESSES** section above for information on where to submit comments.

NPRM-Specific Request for Comments

1. TSA is requesting comments on the impact of regulations and requirements

being imposed by other Federal, State, and Local entities, including DHS components, and potential options for regulatory harmonization.

2. TSA is requesting comments on whether proposed requirements for supply chain risk management should also include requirements to ensure that any new software purchased for, or to be installed on, Critical Cyber Systems meets CISA's Secure-by-Design and Secure-by-Default principles.

3. TSA is requesting comments on existing training and certification programs that could provide low-cost options to meet proposed qualification requirements for Cybersecurity Coordinators. If identified and determined by TSA to be sufficient, TSA could recognize them as examples for owner/operators that would be subject to these requirements.

4. TSA is proposing to require owner/operators to have a Cybersecurity Assessment Plan (CAP) to annually assess and audit the effectiveness of their TSA-approved Cybersecurity Operational Implementation Plan (COIP). TSA is requesting comments on methodologies owner/operators could use to develop a plan that would meet the required annual minimum for assessments and audits, assessment and auditing capabilities that could be included in the CAP, and other options and resources that could ensure a robust auditing and assessment program that provides frequent and regular reviews of effectiveness of CRM program implementation.

5. TSA is requesting comments from pipeline owner/operators on opportunities to streamline compliance and reduce redundancies and duplication of efforts for pipeline facilities regulated under 33 CFR 105.105(a) or 106.105(a).

6. TSA is requesting comment on whether accountable executives and Cybersecurity Coordinators, for all covered owner/operators, should be required to undergo a TSA-conducted Security Threat Assessment (STA), which would include a terrorism/other analyses check, an immigration check, and a criminal history records

check (CHRC).

7. TSA is requesting comment on whether TSA should require all frontline workers ("security-sensitive employees") in the pipeline industry to also be vetted by TSA. Although TSA is not proposing this requirement, TSA seeks comments on how the vetting would impact their operations and costs, and specifically how many employees the entity has that would likely be considered security-sensitive employees.[1]

8. TSA is requesting comment on the inputs used in the Regulatory Impact Analysis (RIA), including those related to the Security Directives (SDs), their implementation, and associated costs and benefits. Comments that will provide the most assistance to TSA will reference a specific portion of this proposed rule, explain the reason for any suggestions or recommended changes, and include data, information, or authority that supports such suggestion or recommended change.

9. TSA invites all interested parties to submit data and information regarding the potential economic impact on small entities that would result from the adoption of the requirements in the proposed rule.

10. TSA invites comments on the proposed collection of information and estimates of burden.

Submitting Comments on the NPRM

With each comment, please identify the docket number at the beginning of your comments. You may submit comments and material electronically, by mail, or fax as provided under **ADDRESSES**, but please submit your comments and material by only one means. If you submit comments by mail or in person, submit them in an unbound format, no larger than 8.5 by 11 inches, suitable for copying and electronic filing.

If you would like TSA to acknowledge receipt of comments submitted by mail,

---

[1] Commenters may find it useful to review the functions that TSA considered for determining security-sensitive employees under current Appendix B to 49 CFR part 1580, Appendix B to part 1582, and Appendix B to part 1584.

include with your comments a self-addressed, stamped postcard or envelope on which the docket number appears, and we will mail it to you.

All comments, except those that include confidential or SSI[2] will be posted to https://www.regulations.gov and include any personal information you have provided. Should you wish your personally identifiable information redacted prior to filing in the docket, please clearly indicate this request in your submission. TSA will consider all comments that are in the docket on or before the closing date for comments and will consider comments filed late to the extent practicable. The docket is available for public inspection before and after the comment closing date.

Submitting Comments on the Proposed Information Collections

Comments on the proposed information collections included in this NPRM should be submitted both to TSA, as indicated above, and to the Office of Information and Regulatory Affairs, Office of Management and Budget (OMB). Comments should be identified by the appropriate OMB Control Number(s) or the title of this proposed rule, addressed to the Desk Officer for the Department of Homeland Security, Transportation Security Administration, and sent via electronic mail to *dhsdeskofficer@omb.eop.gov.*

Handling of Confidential or Proprietary Information and SSI Submitted in Public Comments

Do not submit comments that include trade secrets, confidential commercial or financial information, or SSI to the public regulatory docket. Please submit such comments separately from other comments on the rulemaking. Comments containing this type of information should be appropriately marked as containing such information and submitted by mail to the address listed in the **FOR FURTHER INFORMATION**

[2] "Sensitive Security Information" or "SSI" is information obtained or developed in the conduct of security activities, the disclosure of which would constitute an unwarranted invasion of privacy, reveal trade secrets or privileged or confidential information, or be detrimental to the security of transportation. The protection of SSI is governed by 49 CFR part 1520.

CONTACT section. TSA will take the following actions for all submissions containing SSI:

- TSA will not place comments containing SSI in the public docket and will handle them with applicable safeguards and restrictions on access.
- TSA will hold documents containing SSI, confidential business information, or trade secrets in a separate file to which the public does not have access.
- TSA will place a note in the public docket explaining that commenters have submitted such documents.
- TSA may include a redacted version of the comment in the public docket.
- TSA will treat requests to examine or copy information that is not in the public docket as any other request under the Freedom of Information Act (5 U.S.C. 552) and the Department of Homeland Security (DHS) Freedom of Information Act regulation found in 6 CFR part 5.

Reviewing Comments in the Docket

Please be aware that anyone can search the electronic form of all comments in any of our dockets by the name of the individual, association, business entity, labor union, *etc*., who submitted the comment. For more about privacy and the docket, review the Privacy and Security Notice for the FDMS at https://www.regulations.gov/privacy-notice, as well as the System of Records Notice DOT/ALL 14 – Federal Docket Management System (73 FR 3316, January 17, 2008) and the System of Records Notice DHS/ALL 044 – eRulemaking (85 FR 14226, March 11, 2020).

You may review TSA's electronic public docket at https://www.regulations.gov. In addition, DOT's Docket Management Facility provides a physical facility, staff, equipment, and assistance to the public. To obtain assistance or to review comments in TSA's public docket, you may visit this facility between 9 a.m. and 5 p.m., Monday through Friday, excluding legal holidays, or call (202) 366-9826. This DOT facility is in

the West Building Ground Floor, Room W12-140 at 1200 New Jersey Avenue SE, Washington, DC 20590.

Availability of Rulemaking Document

You can find an electronic copy of this rulemaking using the Internet by accessing the Government Publishing Office's web page at https://www.govinfo.gov/app/collection/FR/to view the daily published *Federal Register* edition or accessing the Office of the Federal Register's web page at https://www.federalregister.gov. Copies are also available by contacting the individual identified for "General Questions" in the **FOR FURTHER INFORMATION CONTACT** section.

Abbreviations and terms used in this document

9/11 Act – Implementing Recommendations of the 9/11 Commission Act of 2007

AAR – Association of American Railroads

Amtrak – National Railroad Passenger Corporation

APTA – American Public Transportation Association

ATSA – Aviation and Transportation Security Act

BOS – Back Office Server

BES – Bulk Electric System

CAP – Cybersecurity Assessment Plan

CEQ – Council on Environmental Quality

CSF – Cybersecurity Framework 2.0

CIRCIA – Cyber Incident Reporting for Critical Infrastructure Act of 2022

CIP – Cybersecurity Implementation Plan

CIRP – Cybersecurity Incident Response Plan

CISA – Cybersecurity and Infrastructure Security Agency

COIP – Cybersecurity Operational Implementation Plan

CPGs – Cross-Sector Cybersecurity Performance Goals

CRM – Cybersecurity risk management

DFAR – Defense Federal Acquisition Regulation Supplement

DHS – Department of Homeland Security

DoD – Department of Defense

DOE – Department of Energy

DOT – Department of Transportation

E.O. – Executive Order

FDMS – Federal Docket Management System

FERC – Federal Energy Regulatory Commission

FISMA – Federal Information Security Modernization Act of 2014

FR – Federal Register

FRA – Federal Railroad Administration

FSB – Russian Federal Security Service

GPS – Global Positioning System

HSIN – Homeland Security Information Network

IC – Information Circular

ICS – Industrial control system

IRFA – Initial Regulatory Flexibility Analysis

IT – Information technology

MFA – Multi-factor authentication

NARA – National Archives and Records Administration

NEPA – National Environmental Policy Act

NERC – National American Electrical Reliability Corporation

NIST – National Institute of Standards and Technology

NPRM – Notice of proposed rulemaking

OMB – Office of Management and Budget

OT – Operational technology

OTRB – Over-the-road bus

PHMSA – Pipeline and Hazardous Materials Safety Administration

POAM – Plan of Action and Milestones

PTC – Positive Train Control

PTPR – Public Transportation and Passenger Railroads

RFA – Regulatory Flexibility Act of 1980

RIA – Regulatory Impact Analysis

SCADA – Supervisory control and data acquisition

SD – Security Directive

SDDCTEA – US Army Military Surface Deployment and Distribution Command Transportation Engineering Agency

SOAR – Security orchestration, automation, and response

SP – Special Publication

SRP – Secure Regulatory Portal

SSI – Sensitive security information

STA – Security threat assessment

STRACNET – Strategic Rail Corridor Network

TSA – Transportation Security Administration

UMRA – Unfunded Mandates Reform Act of 1995

VADR – Validated Architecture Design Review

Table of Contents

I. Executive Summary

A. Purpose of the regulatory action

B. Summary of the major provisions

C. Costs

D. Benefits

II. Background

A. Context

1. Pipeline transportation

2. Rail transportation

a. Freight railroads

b. Passenger railroads

c. Rail transit

3. Cybersecurity threats

4. Threat of cybersecurity incidents at the nexus of IT and OT systems

B. Statutory authorities

1. TSA surface-related SDs and Information Circulars

2. TSA's assessments, guidelines, and regulations applicable to pipeline and rail systems

a. Pipeline guidelines, assessments, and regulations

b. Regulating railroads, public transportation systems, and OTRBs.

C. References

1. National Cybersecurity Strategy

2. NIST Cybersecurity Framework

3. CISA Cross-Sector Cybersecurity Performance Goals

4. TSA's advance notice of proposed rulemaking

a. General support and need for regulatory harmonization and performance-based regulation

b. Core elements

c. Training

d. Supply Chain

e. Third-Party Assessors

5. Regulatory harmonization

III. Proposed Rule

A. Rule organization

1. Cybersecurity requirements

2. Physical security requirements

3. General procedures for security programs, SDs, and Information Circulars

4. Relation to other rulemakings

B. Terms

1. General terms

2. TSA Cybersecurity Lexicon

C. Cybersecurity Risk Management Program—General

1. Introduction

2. Applicability

a. Freight railroads subject to CRM program requirements in proposed subpart D of part 1580

b. Public transportation agencies and passenger railroads subject to CRM program requirements in proposed subpart C of part 1582

c. OTRB owner/operators subject to cybersecurity incident reporting requirements in proposed § 1584.107

d. Pipeline systems and facilities subject to physical security requirements in proposed subpart B of part 1586 and CRM program requirements in proposed subpart C of part 1586

e. Determinations of applicability for requirements in the proposed rule

3. Structure of CRM program requirements (proposed §§ 1580.303, 1582.203, and 1586.203)

D. Specific CRM program requirements

1. Cybersecurity evaluation (proposed §§ 1580.305, 1582.205, and 1586.205)

2. Cybersecurity Operational Implementation Plan (proposed §§ 1580.307, 1582.207, and 1586.207)

a. General COIP requirements

b. Governance of the CRM program (proposed §§ 1580.309, 1580.311, 1582.209, 1582.211, 1586.209, and 1586.211)

c. Identification of Critical Cyber Systems, network architecture, and interdependencies

d. Procedures, policies, and capabilities to protect Critical Cyber Systems

e. Procedures, policies, and capabilities to detect cybersecurity incidents (proposed §§ 1580.321, 1582.221, and 1586.221)

f. Procedures, policies, and capabilities to respond to, and recover from, cybersecurity incidents

3. Cybersecurity Assessment Plan (proposed §§ 1580.329, 1582.229, and 1586.229)

4. Documentation to establish compliance (proposed §§ 1580.331, 1582.231, and 1586.231)

E. Physical security

F. General procedures for security programs, SDs, and Information Circulars

1. General procedures for security programs (proposed revisions to subpart B of part 1570)

2. SDs and Information Circulars (proposed subpart C of part 1570)

3. Exhaustion of administrative remedies (proposed § 1570.119)

4. Severability

5. Enforcement and compliance

G. Summary of applicability and requirements

H. Compliance deadlines and documentation

I. Sensitive Security Information

1. Scope of the revision to TSA's SSI regulatory requirements

2. Disclosure of SSI upon the "need to know"

IV. Regulatory Analyses

A. Economic Impact Analysis

1. Summary of Regulatory Impact Analysis

2. Assessments required by E.O.s 12866 and 13563

a. Costs

b. Cost Sensitivity Analysis

c. Benefits

d. Break-even Analysis

3. OMB A–4 Statement

4. Alternatives considered

5. Regulatory Flexibility Assessment

6. International trade impact assessment

7. Unfunded mandates assessment

B. Paperwork Reduction Act

C. Federalism (E.O. 13132)

D. Energy impact analysis (E.O. 13211)

E. Environmental analysis

F. Tribal consultation (E.O. 13175)

I. Executive Summary

A. Purpose of the regulatory action

On May 8, 2021, a Russian-based cybercriminal group, DarkSide, conducted a ransomware attack[3] that forced a major pipeline company to go offline, resulting in a weeklong shutdown of 5,500 miles of petroleum pipelines on the East Coast. Actions taken to protect the Operational Technology (OT) system temporarily disrupted critical supplies of gasoline and other refined petroleum products throughout the East Coast, resulting in a regional emergency declaration.[4] Some news agencies reported pictures of snaking lines of cars at gas stations across the eastern seaboard and panicked Americans filling bags with fuel, fearing not being able to get to work or get their kids to school. TSA subsequently used its emergency authority under 49 U.S.C. 114(*l*) to impose cybersecurity requirements on certain surface transportation entities. *See* discussion in section II.B.

The cyber threat to the country's critical infrastructure has only increased in the time since TSA initially issued SDs to address cybersecurity in surface transportation in 2021. Cyber threats to surface transportation systems continue to proliferate, as both nation-states and criminal cyber groups target critical infrastructure in order to cause operational disruption and economic harm.[5] Cyber attackers have also maliciously

---

[3] *See* definition of "ransomware" in 6 U.S.C. 650(22).

[4] *See, e.g.*, U.S. Department of Transportation, Federal Motor Carrier Safety Administration, ESC-SSC-WSC - Regional Emergency Declaration 2021-002 - 05-09-2021 (May 9, 2021), available at https://www.fmcsa.dot.gov/emergency/esc-ssc-wsc-regional-emergency-declaration-2021-002-05-09-2021 (last accessed Aug. 1, 2024).

[5] Annual Threat Assessment of the U.S. Intelligence Community, Office of the Director of National Intelligence (2024 Intelligence Community Assessment), 11, 16 (Feb. 5, 2024), available at https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf (last accessed July 23, 2024). Note: Infrastructure references in this 2024 assessment include pipelines.

targeted other surface transportation modes in the United States, including freight railroads, passenger railroads, and rail transit systems, with multiple cyberattack and cyber espionage campaigns.[6] Cybersecurity incidents, particularly ransomware attacks, are likely to increase in the near and long term, due in part to vulnerabilities identified by threat actors in U.S. networks.[7] Especially in light of the ongoing Russia-Ukraine conflict, these threats remain elevated and pose a risk to the national and economic security of the United States.

In its 2023 annual assessment, the Intelligence Community noted that "China almost certainly is capable of launching cyber-attacks that could disrupt critical infrastructure services within the United States, including against oil and gas pipelines, and rail systems."[8] Notably, "[i]f Beijing believed that a major conflict with the United States were imminent, it almost certainly would consider aggressive cyber operations against U.S. homeland critical infrastructure and military assets worldwide. Such a strike would be designed to deter U.S. military action by impeding U.S. decision-making, inducing societal panic, and interfering with the deployment of U.S. forces."[9] In addition, "Russia maintains its ability to target critical infrastructure . . . in the United States as well as in allied and partner countries" and "Tehran's opportunistic approach to cyber-attacks puts U.S. infrastructure at risk for being targeted."[10] Furthermore, "malicious cyber actors have begun testing the capabilities of AI-developed malware

---

[6] These activities include the January 2023 breach of the Washington Metropolitan Area Transit Authority; the January 2023 breach of San Francisco's Bay Area Rapid Transit System; and the April 2021 breach of New York City's Metropolitan Transportation Authority (the nation's largest mass transit agency) by hackers linked to the Chinese government. This threat is ongoing: on February 7, 2024, CISA published an advisory warning of the threat posed by PRC state-sponsored actors. *See* Cybersecurity Advisory (AA24-038A), *PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure*, released by CISA on Feb. 7, 2024.

[7] Alert (AA22-040A), *2021 Trends Show Increased Globalized Threat of Ransomware*, released by CISA on February 10, 2022 (as revised).

[8] Annual Threat Assessment of the U.S. Intelligence Community, Office of the Director of National Intelligence (2023) (2023 Intelligence Community Assessment), 10 (Feb. 6, 2023), available at https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf (last accessed July 23, 2024).

[9] 2023 Intelligence Community Assessment at 10.

[10] 2024 Intelligence Community Assessment at 11.

and AI-assisted software development—technologies that have the potential to enable larger scale, faster, efficient, and more evasive cyber-attacks—against targets, including pipelines, railways, and other US critical infrastructure."[11]

While TSA had issued recommendations to strengthen the cybersecurity of pipeline facilities and systems, *see* discussion in Section II.B.2. of this NPRM, reliance on voluntary actions may not be sufficient in light of the cyber threat to our national and economic security. As noted in the National Cybersecurity Strategy, "While voluntary approaches to critical infrastructure cybersecurity have produced meaningful improvements, the lack of mandatory requirements has resulted in inadequate and inconsistent outcomes. Today's marketplace insufficiently rewards—and often disadvantages—the owners and operators of critical infrastructure who invest in proactive measures to prevent or mitigate the effects of cyber incidents."[12]

The requirements proposed in this rule would strengthen cybersecurity and resiliency for the surface transportation sector by mandating reporting of cybersecurity incidents and development of a robust CRM program. This rulemaking builds upon TSA's previously issued requirements and recommendations, the cybersecurity framework (CSF) developed by the National Institute of Standards and Technology (NIST),[13] and the Cross-Sector Cybersecurity Performance Goals (CPGs) developed by the Cybersecurity and Infrastructure Security Agency (CISA).[14]

B. Summary of the major provisions

This NPRM proposes to require owner/operators[15] of designated freight railroads,

---

[11] DHS Intelligence and Analysis (I&A), Homeland Threat Assessment 18 (2024), available at https://www.dhs.gov/sites/default/files/2023-09/23_0913_ia_23-333-ia_u_homeland-threat-assessment-2024_508C_V6_13Sep23.pdf (last accessed July 23, 2024).
[12] *See* National Cybersecurity Strategy at 8 (March 2023), available at https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf (last accessed July 29, 2024).
[13] *See* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf (last accessed May 5, 2024) for more information on the NIST Cybersecurity Framework (CSF) 2.0.
[14] *See* https://www.cisa.gov/cross-sector-cybersecurity-performance-goals (last accessed Sept. 22, 2023) for more information on the CPGs. A table that aligns the NIST CSF, CPGs, and proposed requirements is available in the docket for this rulemaking.
[15] *See* 49 CFR 1500.3 for the definition of "owner/operators" as used in this rulemaking.

passenger railroads, rail transit, and pipeline facilities and/or systems to have a CRM program approved by TSA. The proposed CRM program includes three primary elements. First, owner/operators to whom the proposed rule applies would be required to annually conduct an enterprise-wide cybersecurity evaluation that would identify the current profile of cybersecurity (including physical and logical/virtual controls) compared to the target profile. The target profile must, at a minimum, include the security outcomes identified in the proposed rule and should also consider recommendations in the NIST CSF.[16]

Second, those owner/operators would be required to develop a COIP that includes the following information: (a) identification of individuals/positions responsible for the governance of the owner/operator's CRM program, including an accountable executive and Cybersecurity Coordinator(s); (b) identification of Critical Cyber Systems, specific network architecture issues, and baseline communications; (c) detailed measures to protect these Critical Cyber Systems; (d) detailed measures to detect cybersecurity incidents and monitor these Critical Cyber Systems; and (e) measures to address response to, and recovery from, a cybersecurity incident. Although many of these measures for the COIP are limited to Critical Cyber Systems, all owner/operators within the proposed scope of applicability would be required to have a Cybersecurity Incident Response Plan (CIRP), regardless of whether they identify any Critical Cyber Systems.

Third, owner/operators subject to the proposed rule would be required to have a CAP that includes a schedule for assessments, an annual report of assessment results, and identification of unaddressed vulnerabilities. Owner/operators would also be required to ensure any individuals or companies assigned or hired to evaluate the effectiveness of the owner/operator's CRM program are independent, *i.e.*, do not have a personal, financial interest in the results of the assessment.

---

[16] *See* NIST CSF, *supra* note 13.

As part of this rule, TSA also is proposing to reorganize requirements in subchapter D of 49 CFR chapter XII related to security coordinators, reporting significant security concerns, and security training of security-sensitive employees. TSA would move these requirements from 49 CFR part 1570 and add them to the specific modal requirements in parts 1580, 1582, 1584, and a new part 1586, which is applicable to pipeline systems and facilities.[17] In general, the applicability of proposed requirements related to designation of a cybersecurity coordinator and reporting cybersecurity incidents align with the current requirements for designation of a (physical) security coordinator and reporting of significant (physical) security concerns under 49 CFR part 1570.201 and 1570.203.

TSA is also proposing to distinguish between requirements focused on physical security and those focused on cybersecurity. As part of this reorganization and proposed imposition of new cybersecurity requirements, TSA is proposing that all owner/operators currently required to report significant security concerns to TSA, under current 49 CFR 1570.203,[18] report significant physical security concerns to TSA and report cybersecurity incidents to CISA. TSA is proposing that owner/operators of designated pipeline facilities and systems also report both physical and cybersecurity incidents.

Finally, TSA is proposing to incorporate into subchapter D a new section related to issuance of SDs and Information Circulars (ICs), mirroring language currently applicable in the aviation industry. Adding this section would ensure consistent procedures for issuance of SDs and ICs across all modes of transportation subject to TSA's authorities.

C. Costs

[17] TSA may make related revisions to organization of a rulemaking that would finalize proposed requirements in the NPRM, Vetting of Certain Surface Transportation Employees, 88 FR 33472 (May 23, 2023).

[18] *See also* Appendix A to 49 CFR part 1570.

TSA estimates the proposed rule would impact just under 300 surface transportation owner/operators. Using the risk-based criteria for application discussed below, *see* Section III.C.2., TSA estimates these proposed requirements would apply to 73 of the approximately 620 freight railroads currently operating in the United States; 34 of the approximately 92 public transportation agencies and passenger railroads (PTPR) operating in the United States; 71 OTRB owner/operators who are currently subject to TSA's regulatory requirements to report significant security concerns; and 115 of the approximately 2,105 pipeline facilities and systems subject to safety regulations issued by the Pipeline and Hazardous Materials Safety Administration (PHMSA), as codified in 49 CFR part 192 and 49 CFR 195.1.[19]

Table 1 identifies TSA's estimates for the overall cost of this proposed rule. This table captures the industry's costs associated with implementing the proposed requirements as well as TSA's costs for overseeing implementation, over a 10-year period of analysis. *See* Section IV of this NPRM and the related Regulatory Impact Analysis for a more detailed breakdown of the estimated costs.

TABLE 1: COST OF FINAL RULE

	Estimated Costs (over 10 years, discounted at 7 percent)
Freight Railroads	$685,776,600
Passenger Railroads and Rail Transit	881,136,800
OTRBs	215,900
Pipeline Facilities and Systems	580,183,200
TSA	14,241,200
Total	$2,161,553,800
Annualized	$307,756,600

D. Benefits

The primary benefit of the proposed rule is a potential reduction in the risk of a successful attack or cybersecurity incident and the impact of such incidents as a result of implementing the proposed requirements. Implementation of a CRM program, as

[19] The proposed applicability for pipeline facilities and systems specifically excludes U.S. facilities specified in 33 CFR 105.105(a) that are regulated under 33 CFR part 105 or facilities specified in 33 CFR 106.105(a) that are regulated under 33 CFR part 106.

described under the proposed rule, could help enhance the security of the regulated population by improving the owner/operator's ability to identify, detect, protect against, respond to, and recover from cybersecurity incidents.

The proposed cybersecurity outcomes this rule would require provide owner/operators with a blueprint for improving defenses against cybersecurity incidents. Industry experience indicates that having a defense-in-depth approach to cybersecurity enhances the ability to prevent and respond to breaches of operational systems and compromises of sensitive information.[20] TSA anticipates the proposed rule's requirements, such as enhancing system security, maintaining backups, monitoring systems, and developing a response plan, would strengthen cybersecurity defenses over the long term. For instance, depending on the individual circumstances of a given cyber-attack or cybersecurity incident—

- A commitment to patch management, system segmentation, and firewalls could limit the resources potential malicious actors would be able to access during an intrusion;[21]
- The presence of backups could allow for system restoration, data recovery, and unhindered system operations;[22]
- Continuous monitoring of the network could help to detect and respond to potential threats and limit system degradation[23] and

[20] Well-designed security systems have been credited for limiting damages in recent cyber incident cases: *See* ABC7 New York, Hackers breached several of MTA's computer systems in April (June 2, 2021), available at https://abc7ny.com/mta-hack-computer-nyc-new-york-city/10734358/ (last accessed Sept. 28, 2023).
[21] *See, e.g.,* outcomes associated with the following CISA CPGs available at https://www.cisa.gov/cross-sector-cybersecurity-performance-goals (last accessed June 10, 2024): CISA CPG 1.E.
[22] *See, e.g., id.* at CISA CPG 2.R.
[23] *See, e.g., id.* at CISA CPGs 2.A, 2.F., 2.G. and 3.A.

- Having a response plan in place in case of a successful cyber-attack or cybersecurity incident would reduce its impact, build in resiliency, and support rapid resumption of normal operations.[24]

These enhances, in turn, could reduce the chance of negative consequences and service interruptions from cybersecurity incidents to the benefit of owners/operators, passengers, and consumers.

II. Background

A. Context

1. Pipeline transportation

The national pipeline system consists of more than 2.9 million miles of networked pipelines transporting hazardous liquids, natural gas, and other liquids and gases for energy needs and manufacturing.[25] Although most pipeline infrastructure is buried underground, operational elements such as compressors, metering, regulating, pumping stations, aerial crossings, and breakout tanks are typically located above ground. Under operating pressure, the pipeline system is used as a conveyance to deliver resources from one location to another. In addition to portions of the network that are manually operated, the pipeline system includes use of automated industrial control systems (ICS), such as supervisory control and data acquisition (SCADA) systems to monitor and manage pipeline operations. These systems use remote sensors, signals, and preprogramed parameters to activate valves and pumps to maintain product flows within tolerances. Pipeline systems supply energy commodities and raw materials across the country to utilities, airports, military sites, and to the nation's industrial and manufacturing sectors. Protecting the vital supply chain infrastructure of pipeline operations is critical to national security and commerce.

---

[24] *See, e.g., id.* at CISA CPGs 2.O, 2.P, 2.R., 2.S., and 2.T.

[25] Mileage information is available at https://www.phmsa.dot.gov/data-and-statistics/pipeline/annual-report-mileage-summary-statistics (last accessed Nov. 30, 2023).

2. Rail transportation

The rail transportation sector includes freight railroads, passenger railroads (including inter-city and commuter), and rail transit.

a. Freight railroads

The national freight rail network is a complex system that includes both physical and cyber infrastructure and consists of more than 620 freight railroads operating across nearly 140,000 rail miles. This sector includes six Class I railroads,[26] local (also known as Short Line) railroads, and regional railroads. The Class I railroads had a calendar year 2021 operating revenues of at least $900 million. These six railroads also account for approximately 68 percent of freight rail mileage, 88 percent of employees, and 94 percent of revenue. Regional railroads and local railroads range in size from operations handling a few carloads monthly to multi-state operators nearly the size of a Class I operation.[27] As stated by the Association of American Railroads (AAR), the freight rail sector provides "a safe, efficient, and cost-effective transportation network that reliably serves customers and the nation's economy."[28]

Freight railroads are private entities that own and are responsible for their own infrastructure.[29] They maintain the locomotives, rolling stock, and fixed assets involved in the transportation of goods and materials across the nation's rail system. As required by Congress, railroads are subject to safety regulations promulgated and enforced by the Federal Railroad Administration (FRA). TSA administers and enforces the rail security regulations in 49 CFR part 1580.

b. Passenger railroads

---

[26] For purposes of TSA's regulations, "Class I" means "Class I" as assigned by regulations of the Surface Transportation Board (STB) (49 CFR part 1201; General Instructions 1-1). *See also infra* note 123.
[27] *See* https://www.aar.org/wp-content/uploads/2020/08/AAR-Railroad-101-Freight-Railroads-Fact-Sheet.pdf (May 2023 update, last accessed June 3, 2023).
[28] *Id.*
[29] *Id.*

Passenger rail is divided into two categories: inter-city and commuter rail service. Inter-city provides long-distance service, while commuter railroads provide service over shorter distances, usually less than 100 miles. The National Railroad Passenger Corporation (Amtrak) is the sole long-distance inter-city passenger railroad in the contiguous United States. Amtrak, which had a pre-pandemic annual ridership of approximately 31.7 million, operates a nationwide rail network, serving more than 500 destinations in 46 states, the District of Columbia, and three Canadian provinces on more than 21,300 track-miles.[30] Nearly half of all Amtrak trains operate at top speeds of 100 mph or greater. In fiscal year 2023, Amtrak customers took nearly 28.6 million trips, up 24 percent over the previous year.[31] In addition to inter-city service, Amtrak is one of the largest operators of contract commuter services in North America, providing services and/or infrastructure access to 13 state and regional authorities.[32]

Freight railroads provide the tracks for most passenger rail operations. For example, 71 percent of the track on which Amtrak operates is owned by other railroads. These "host railroads" include large, publicly traded freight rail companies in the U.S. or Canada, State and Local government agencies, and small businesses. Amtrak pays the host railroads for use of their track and other resources as needed.[33]

Amtrak and other passenger rail agencies, however, are not wholly dependent on freight rail infrastructure and corridors for operational feasibility; they sometimes control, operate, and maintain tracks, facilities, construction sites, utilities, and computerized networks essential to their own operations. For example, the Northeast Corridor is an electrified railway line in the Northeast megalopolis of the United States owned primarily

---

[30] *See* https://www.apta.com/wp-content/uploads/APTA_Fact-Book-2019_FINAL.pdf (last accessed Sept. 19, 2022).
[31] *See* https://media.amtrak.com/2023/11/amtrak-fiscal-year-2023-ridership-exceeds-expectations-as-demand-for-passenger-rail-soars/ (last accessed July 30, 2024).
[32] *See* https://www.amtrak.com/content/dam/projects/dotcom/english/public/documents/corporate/nationalfactsheets/Amtrak-Company-Profile-FY2023-041824.pdf. at 4 (last accessed July 30, 2024).
[33] *Id.* at 2.

by Amtrak. It runs from Boston through New York City, Philadelphia, and Baltimore, with a terminus in Washington, D.C. The majority of this corridor, 263 of the 457 route-miles of the main line, are owned and operated by Amtrak.[34]

Amtrak and other passenger railroads also host freight rail operations. In fact, the Northeast Corridor is the busiest railroad in North America, with approximately 2,000 Amtrak, commuter, and freight trains operating over some portion of the Washington-Boston route each day.[35] As with freight railroads, passenger railroads are subject to safety regulations put forth and enforced by the FRA. TSA administers and enforces passenger rail security regulations in 49 CFR part 1582.

c. Rail transit

Public transportation in America is critically important to our way of life, as evidenced by the number of riders on the nation's public transportation systems. According to the American Public Transportation Association (APTA), 2022 Public Transportation Fact Book, there were over 4.49 billion unlinked passenger trips in 2021.[36] Nationwide, 5.0 million Americans commute to work on transit, equivalent to approximately 3.1 percent of workers. In major metropolitan areas, like New York City, over 27 percent of commuters rely on public transportation for their daily commute.[37] Rail transit is a critical part of this system. According to APTA, 87 percent of trips on transit directly benefit the local economy, including 50 percent of trips to and from work and 37 percent of trips are for shopping and recreational spending.[38] A successful cyber-attack would have a profound impact on ridership and a negative economic impact

---

[34] *Id.* at 4.
[35] *Id.*
[36] *See* APTA, 2023 Public Transportation Fact Book at 3, available at https://www.apta.com/wp-content/uploads/APTA-2023-Public-Transportation-Fact-Book.pdf (last accessed July 30, 2024). Unlinked passenger trips are an industry measure of ridership, with a trip being defined as any time a person boards a transit vehicle, including transfers.
[37] *Id.* at 12.
[38] *Id.* at 3. Rail transit includes heavy rail systems, often referred to as "subways" or "metros" that do not interact with traffic; light rail and streetcars, often referred to as "surface rail," that may operate on streets, with or without their own dedicated lanes; and commuter rail services that are higher-speed, higher-capacity trains with less-frequent stops.

nationwide. TSA administers and enforces rail transit security regulations in 49 CFR part 1582.

3. Cybersecurity threats

Threat actors have demonstrated their willingness to engage in cyber intrusions and conduct cybersecurity incidents against critical infrastructure by exploiting vulnerabilities in OT[39] and Information Technology (IT)[40] systems. Pipeline and rail systems, and associated facilities, may be vulnerable to cybersecurity incidents due to legacy ICS that lack updated security controls and the dispersed nature of pipeline and rail networks spanning urban and outlying areas.[41]

As pipeline and rail owner/operators have begun to integrate IT and OT systems into their operating environment to further improve safety, enable efficiencies, and/or increase automation, their operations become increasingly vulnerable to new and evolving cyber threats. A successful cyber-intrusion could affect the safe operation and reliability of OT systems, including SCADA systems, process control systems, distributed control systems, safety control systems, measurement systems, and telemetry systems.

From a design perspective, some pipeline and rail assets are more attractive to targets for a cybersecurity incident simply because of the transported commodity and the impact an incident would have on national security and commerce. Minor pipeline and

---

[39] For purposes of this NPRM, TSA defines an "OT system" as "a general term that encompasses several types of control systems, including industrial control systems, supervisory control and data acquisition systems, distributed control systems, and other control system configurations, such as programmable logic controllers, fire control systems, and physical access control systems, often found in the industrial sector and critical infrastructure. Such systems consist of combinations of programmable electrical, mechanical, hydraulic, pneumatic devices or systems that interact with the physical environment or manage devices that interact with the physical environment."

[40] For purposes of this NPRM, TSA defines an "IT System" as "any services, equipment, or interconnected systems or subsystems of equipment that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information that fall within the responsibility of owner/operator to operate and/or maintain."

[41] *See* CISA, *Securing Industrial Control Systems: A Unified Initiative (FY 2019-2023)* at 4, available at https://www.cisa.gov/sites/default/files/publications/Securing_Industrial_Control_Systems_S508C.pdf (last accessed Aug. 30, 2023).

rail system disruptions may result in commodity price increases, while prolonged pipeline and rail operational disruptions could lead to widespread energy shortages and disruption of critical supply lines. Short-and long-term disruptions and delays may affect other domestic critical infrastructure and industries, such as our national defense system, that depend on pipeline and rail system commodities, such as our national defense system.

The May 2021 DarkSide attack on a major pipeline company is just one of many recent ransomware attacks that have demonstrated the necessity of ensuring that critical infrastructure owner/operators are proactively deploying CRM measures. The Multi-State Information Sharing and Analysis Center observed a 153 percent increase in the number of ransomware attacks reported by State, Local, Tribal, and Territorial governments in the one-year period from 2018 to 2019, including both opportunistic and strategic campaigns.[42] The need to mitigate the threats facing domestic critical infrastructure, including by enhancing the pipeline and rail industry's current cybersecurity risk management posture, is further highlighted by recent warnings about Russian,[43] Chinese,[44] and Iranian[45] state-sponsored cyber espionage campaigns to develop capabilities to disrupt U.S. critical infrastructure to include the transportation sector.[46] Failure to take action could have significant implications for national and economic security.

On March 24, 2022, the U.S. Department of Justice unsealed indictments of three

---

[42] *See* MS-ISAC Security Primer 2020-0002 (May 2020), available at https://www.cisecurity.org/insights/white-papers/security-primer-ransomware (last accessed June 3, 2023).
[43] *See* 2023 Intelligence Community Assessment, *supra* note 9, at 15.
[44] *See id.* at 10
[45] *See id.* at 19.
[46] In addition to the resources available at the cites referenced in the preceding notes, additional information is available on CISA's advisories organized by state-sponsored groups, *i.e.*, https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/china (China Cyber Threat Overview and Advisories); https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/russia (Russian Cyber Threat Overview and Advisories); and https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/iran (Iran Cyber Threat Overview and Advisories). *See also* FBI Private Industry Bulletin *TRITON Malware Remains Threat to Global Critical Infrastructure Industrial Control Systems* (Mar. 24, 2022), available at docs.house.gov/meetings/JU/JU00/20220329/114533/HHRG-117-JU00-20220329-SD009.pdf (last accessed Sept. 22, 2023).

Russian Federal Security Service (FSB) officers and employees of a State Research Center of the Russian Federation Central Scientific Research Institute of Chemistry and Mechanics for their involvement in intrusion campaigns against U.S. and international oil refineries, nuclear facilities, and energy companies. Documents revealed that the Russian FSB conducted a multi-stage campaign in which they gained remote access to U.S. and international Energy Sector networks, deployed ICS-focused malware, and collected and exfiltrated enterprise and ICS-related data.[47] A recent multi-national cybersecurity advisory noted that "Russian state-sponsored cyber actors have demonstrated capabilities to compromise IT networks; develop mechanisms to maintain long-term, persistent access to IT networks; exfiltrate sensitive data from IT and [OT] networks; and disrupt critical (ICS)/OT functions by deploying destructive malware."[48]

The nation's adversaries and strategic competitors will continue to use cyber espionage and cyber-attacks to seek political, economic, and military advantage over the United States and its allies and partners. These recent incidents demonstrate the potentially devastating impact that increasingly sophisticated cybersecurity incidents can have on our nation's critical infrastructure, as well as the direct repercussions felt by U.S. citizens. The consequences and threats discussed above demonstrate the necessity of ensuring that critical infrastructure owner/operators are proactively deploying CRM measures.

4. Threat of cybersecurity incidents at the nexus of IT and OT systems

---

[47] The superseding indictment is available at https://www.justice.gov/opa/pr/us-citizens-and-russian-intelligence-officers-charged-conspiring-use-us-citizens-illegal#:~:text=Among%20other%20illegal%20activities%2C%20the,for%20local%20office%20in%20St. (Department of Justice Press Release, U.S. Citizens and Russian Intelligence Officers Charged with Conspiring to Use U.S. Citizens as Illegal Agents of the Russian Government, Apr. 18, 2023) (last accessed Sept. 25, 2023); *see also* Joint Cybersecurity Advisory, *Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector*, Alert AA22-083A (Mar. 24, 2022), available at https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-083a (last accessed Dec. 29, 2023).

[48] *See* Joint Cybersecurity Advisory, *Russian State Sponsored and Criminal Cyber Threat to Critical Infrastructure*, Alert AA22-110A (Apr. 20, 2022), available at https://www.cisa.gov/uscert/ncas/alerts/aa22-110a (last accessed Dec. 29, 2023).

Some sectors have taken significant steps to protect either their IT or OT systems, depending on which is considered most critical for their business needs (*e.g.,* a commodities sector may focus on OT systems while a financial sector or other business that focuses on data may focus on IT systems). Ransomware attacks targeting critical infrastructure threaten *both* IT and OT systems and exploit the connections between these systems. For example, when OT components are connected to IT networks, this connection provides a path for cyber actors to pivot from IT to OT systems.[49] Given the importance of critical infrastructure to national and economic security, accessible OT systems and their connected assets and control structures are an attractive target for malicious cyber actors seeking to disrupt critical infrastructure for profit or to further other objectives.[50] As CISA notes, recent cybersecurity incidents demonstrate that intrusions affecting IT systems can also affect critical operational processes even if the intrusion does not directly impact an OT system.[51] For example, business operations on the IT system sometimes are used to orchestrate OT system operations. As a result, when there is a compromise of the IT system, there is a risk of unaffected OT systems being impacted by the loss of operational directives and accounting functions.

DHS, the Department of Energy (DOE), the Federal Bureau of Investigation, and the National Security Agency have all urged the private sector to implement a layered, "defense-in-depth" cybersecurity posture. For example, ensuring that OT and IT systems are separate and segregated will help protect against intrusions that can exploit vulnerabilities from one system and move laterally to infect another. A stand-alone, unconnected ("air-gapped") OT system is safer from outside threats than an OT system connected to one or more enterprise IT systems with external connectivity (no matter

---

[49] *See* CISA Fact Sheet, *Rising Ransomware Threat to Operational Technology Assets* (June 2021), available at https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Rising_Ransomware_Threat_to_OT_Assets_508C.pdf (last accessed June 3, 2023).
[50] *Id.*
[51] *Id.*

how secure the outside connections are thought to be).[52] By implementing a layered approach, owner/operators and their network administrators will enhance the defensive cybersecurity posture of their OT and IT systems, reducing the risk of compromise or severe operational degradation if their system is compromised by malicious cyber actors.[53]

The cyber threat to our nation's critical infrastructure has only increased in the time since TSA's first cybersecurity SD was issued. The surface transportation sector, including the oil and gas pipeline industry, is increasingly dependent on automation and use of connected technology.[54] Cyber threats to surface transportation systems continue to proliferate as both nation-state actors and criminal cyber groups are actively targeting oil and natural gas pipelines with the potential to cause operational disruption and economic harm. Ransomware attacks are likely to increase in the near and long term, due in part to vulnerabilities identified by threat actors in U.S. networks, while nation-state actors continue to target U.S. infrastructure for disruptive cyberattack options in a crisis or conflict.[55] These threats and their potential consequences to critical transportation systems and infrastructure demonstrate the need for TSA to ensure owner/operators continue to proactively deploy cybersecurity risk management measures.

Protecting this critical and interconnected sector, and the consumers that rely on it, from the impact of cybersecurity impacts, cannot be accomplished on an ad hoc basis

---

[52] *See* National Security Agency Cybersecurity Advisory, *Stop Malicious Cyber Activity Against Connected Operational Technology* (PP-21-0601 | APR 2021 Ver 1.0), available at https://media.defense.gov/2021/Apr/29/2002630479/-1/-1/1/CSA_STOP-MCA-AGAINST-OT_UOO13672321.PDF (last accessed Sept. 19, 2022).

[53] *See* Joint Cybersecurity Advisory, *Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013* (Alert AA21-200A), available at https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-201a (last accessed Sept. 19, 2024).

[54] *See* written testimony of Eric Goldstein, Executive Assistant Director for Cybersecurity CISA, Joint Hearing Before the Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation, and the Subcommittee on Transportation and Maritime Security, U.S. House of Representatives Committee on Homeland Security, *Cyber Threats in the Pipeline: Lessons from the Federal Response to the Colonial Pipeline Ransomware Attack* (June 15, 2021).

[55] *See* 2023 Intelligence Community Assessment, *supra* note 8, for open-source information on the cybersecurity threat. *See also* 2024 Intelligence Community Assessment, *supra* note 5.

that relies entirely on voluntary action. The pipeline sector is an interconnected system. As noted by the Interstate Natural Gas Association of America, "natural gas transmission systems have numerous interconnection points and market hubs. . . . There are no major interstate pipelines that operate in isolation, *i.e.*, without interconnection with at least one or more other pipelines."[56] As noted by the PHMSA, "[p]ipelines play a vital role in our daily lives. They transport fuels and petrochemical feedstocks that we use in cooking and cleaning, in our daily commutes and travel, in heating our homes and businesses, and in manufacturing hundreds of products we use daily."[57]

Similarly, with the nation's rail system, railroads move over 1.5 billion tons of freight annually,[58] and a disruption to this movement would have damaging ripple effects across industries, including on international trade. In the rail system, the implementation of positive train control (PTC) systems has resulted in a far more interconnected rail system than previously existed in the Unites States. The interoperability of PTC systems occurs when the "controlling locomotives and/or cab cars of any host railroad and tenant railroad operating on the same PTC-equipped main line are able to communicate with and respond to the PTC system, even when train are moving over property boundaries."[59] The nation's economic security relies on freight rail owner/operators to transport critical manufacturing materials, food product, lumber, coal, and other materials critical to the supply chain. These railroads also host major passenger and commuter rail lines.[60] The nature of these systems requires a baseline of cybersecurity risk management across the

---

[56] The Interstate Natural Gas Association of America, *The Interstate Natural Gas Transmission System: Scale, Physical Complexity, and Business Model,* at 1-2 (Aug. 6, 2010).
[57] PHMSA, *Pipeline Basics*, available at https://primis.phmsa.dot.gov/comm/PipelineBasics.htm (last accessed July 29, 2024).
[58] *See* https://www.aar.org/data-center/railroads-states/#:~:text=In%20a%20typical%20year%2C%20U.S.,nearly%20140%2C000%20miles%20of%20track (last accessed July 31, 2024).
[59] *See* https://www.freightwaves.com/news/u-s-class-i-railroads-inch-towards-full-positive-train-control-implementation, *PTC is interoperable on nearly half of the Class I U.S. rail operations* (posted Feb. 28, 2020, by Joanna Marsh) (last accessed July 29, 2024).
[60] *Id.*

highest-risk operations to protect these vital resources to national security, including economic security.

B. Statutory authorities

The security of the nation's transportation systems is vital to the economic health and security of the United States. Ensuring transportation security while promoting the movement of legitimate travelers and commerce is a critical counter-terrorism mission assigned to TSA.

Following the attacks of September 11, 2001, Congress created TSA under the Aviation and Transportation Security Act (ATSA) and established the agency's primary federal role to enhance security for all modes of transportation.[61] The scope of TSA's authority includes assessing security risks,[62] developing security measures to address identified risks,[63] and enforcing compliance with these measures.[64] TSA has broad regulatory authority to issue, rescind, and revise regulations as necessary to carry out its transportation security functions.

1. TSA surface-related SDs and Information Circulars

Under 49 U.S.C. 114(*l*)(2)(A), TSA is authorized to issue emergency regulations or SDs without providing notice or public comment where "the Administrator determines that a regulation or security directive must be issued immediately in order to protect transportation security."[65] SDs issued pursuant to the procedures in 49 U.S.C. 114(*l*)(2)

---

[61] Public Law 107-71, 115 Stat. 597 (Nov. 19, 2001). ATSA created TSA as a component of the DOT. *See* 49 U.S.C. 114, which codified section 101 of ATSA. Section 403(2) of the Homeland Security Act of 2002 (HSA), Public Law 107-296, 116 Stat. 2135 (Nov. 25, 2002), transferred all functions related to transportation security, including those of the Secretary of Transportation and the Under Secretary of Transportation for Security, to the Secretary of Homeland Security. Pursuant to DHS Delegation Number 7060.02.1, the Secretary delegated to the Administrator, subject to the Secretary's guidance and control, the authority vested in the Secretary with respect to TSA, including the authority in sec. 403(2) of the HSA. *See also* 49 U.S.C. 114(d), which specifically gives the Administrator authority over all modes of transportation regulated by the Department of Transportation at the time TSA was established.

[62] *See, e.g.*, 49 U.S.C. 114(f)(1)-(3).

[63] *See, e.g.*, 49 U.S.C. 114(f)(4), (10), and (11).

[64] *See, e.g.*, 49 U.S.C. 114(f)(7) and (9).

[65] This provision states: "Notwithstanding any other provision of law or executive order (including an executive order requiring a cost-benefit analysis), if the Administrator [of TSA] determines that a

"shall remain effective for a period not to exceed 90 days unless ratified or disapproved by the [Transportation Security Oversight] Board [(TSOB)] or rescinded by the Administrator."[66]

TSA issued SDs in 2021 and 2022[67] in response to the cybersecurity threat to surface transportation systems and associated infrastructure to protect against the significant harm to the national and economic security of the United States that could result from the "degradation, destruction, or malfunction of systems that control this infrastructure."[68] The most current and previous versions of these SDs are available on TSA's website.[69]

The first pipeline SD (the SD Pipeline-2021-01 series), issued on May 27, 2021, requires several actions to enhance the security of critical pipeline systems[70] against cybersecurity threats and provided that owners/operators must: (1) designate a primary and alternate Cybersecurity Coordinator; (2) report cybersecurity incidents to CISA within 24 hours of identification of a cybersecurity incident;[71] and (3) review TSA's pipeline guidelines,[72] assess their current cybersecurity posture, and identify remediation measures to address the vulnerabilities and cybersecurity gaps.[73] For purposes of the SDs, TSA defined a "cybersecurity incident" as "an event that, without lawful authority,

---

regulation or security directive must be issued immediately in order to protect transportation security, the Administrator shall issue the regulation or security directive without providing notice or an opportunity for comment and without prior approval of the Secretary." In addition, section 114(d) provides the Administrator authority for security of all modes of transportation; section 114(f) provides specific additional duties and powers to the Administrator; and section 114(m) provides authority for the Administrator to take actions that support other agencies.

[66] 49 U.S.C. 114(*l*)(2)(B).

[67] See https://www.tsa.gov/sd-and-ea (last accessed June 10, 2024). TSA issued these SDs under the specific authority of 49 U.S.C. 114(*l*)(2)(A).

[68] National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems (July 28, 2021).

[69] *See supra* note 67.

[70] "Critical pipeline systems" are determined by TSA based on risk.

[71] As originally issued, the directive required notification within 12 hours of identification. In May 2022, TSA revised this requirement to require notification within 24 hours of identification.

[72] *See* section I.F. for more information on TSA's guidelines for the pipeline owner/operators.

[73] TSA may also use the results of assessments to identify the need to impose additional security measures as appropriate or necessary. TSA and CISA may use the information submitted for vulnerability identification, trend analysis, or to generate anonymized indicators of compromise or other cybersecurity products to prevent other cybersecurity incidents.

jeopardizes, disrupts or otherwise impacts, or is reasonably likely to jeopardize, disrupt or otherwise impact, the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident on the system." The reports must (1) identify the affected systems or facilities; and (2) describe the threat, incident, and impact or potential impact on IT and OT systems and operations.

The second pipeline SD (the SD Pipeline-2021-02 series), first issued on July 19, 2021, required owner/operators to implement specific mitigation measures to protect against ransomware attacks and other known threats to IT and OT systems and conduct a cybersecurity architecture design review. This SD also required owner/operators to develop and adopt a cybersecurity incident response plan to reduce the risk of operational disruption should their IT and/or OT systems be affected by a cybersecurity incident.[74]

In December 2021, TSA issued SDs to higher-risk freight railroads (the SD 1580-21-01 series) and passenger rail and rail transit owner/operators (the SD 1582-21-01 series), requiring that they also implement the following requirements previously imposed on pipeline systems and facilities: (1) designation of a Cybersecurity Coordinator; (2) reporting of cybersecurity incidents to CISA within 24 hours; (3) developing and implementing a cybersecurity incident response plan to reduce the risk of an operational disruption; and (4) completing a cybersecurity vulnerability assessment to identify potential gaps or vulnerabilities in their systems. For owner/operators not specifically covered under the SD 1580-21-01 or 1582-21-01 series, TSA also issued an Information Circular (IC-2021-01), which included a non-binding recommendation for those surface owner/operators not subject to the SDs to voluntarily implement the same

[74] *See* https://www.tsa.gov/sites/default/files/sd_pipeline_2021-02b-non_ssi_06-06-2022.pdf (last accessed June 10, 2024) for a version of the SD with the prescriptive requirements.

measures.[75]

In the year following issuance of the second pipeline SD, TSA determined that its prescriptive requirements limited the ability of owner/operators to adapt the requirements to their operational environment and apply innovative alternative measures and new capabilities. Because of the need to provide greater flexibility, TSA revised this SD series, effective July 27, 2022 (SD Pipeline-2021-02C), to maintain the security objectives in the previous versions of the SD but also provide more flexibility by imposing performance-based, rather than prescriptive, security measures. As revised, the SD allows covered owner/operators to choose how best to implement security measures for their specific systems and operations while mandating that they achieve critical security outcomes. This approach also affords these owner/operators with the ability to adopt new technologies and security capabilities as they become available, if TSA's mandated security outcomes continue to be met.

The current directive, most recently revised in July 2024, specifically requires the covered owner/operators of critical pipeline systems and facilities to take the following actions:

- Establish and implement a TSA-approved CIP that describes the specific cybersecurity measures employed to protect Critical Cyber Systems, as defined by the owner/operator, and the schedule for achieving the security outcomes identified by TSA.
- Develop and maintain an up-to-date CIRP to reduce the risk of operational disruption, or the risk of other business disruption, as defined in the SD, should the IT and/or OT systems of a gas or liquid pipeline or railroad be affected by a cybersecurity incident. The CIRP must be exercised each year

[75] *See* https://www.tsa.gov/sites/default/files/20211201_surface-ic-2021-01.pdf (last accessed Oct. 16, 2023).

to test at least two objectives of the plan and include personnel responsible for actions in the CIRP.

- Develop a CAP that describes how the owner/operator will proactively, regularly, and completely assess the effectiveness of cybersecurity measures in their CIP, and identify and resolve device, network, and/or system vulnerabilities. This plan must be submitted to TSA for approval and an annual report provided to TSA and corporate leadership.

The CIP must identify how the owner/operators meet the following primary security outcomes:

- Implement network segmentation policies and controls to ensure that the OT system can continue to safely operate in the event that an IT system has been compromised, or vice versa;
- Implement access control measures to secure and prevent unauthorized access to critical cyber systems;
- Implement continuous monitoring and detection policies and procedures to detect cybersecurity threats and correct anomalies that affect critical cyber system operations; and
- Reduce the risk of exploitation of unpatched systems through the application of security patches and updates for operating systems, applications, drivers, and firmware on critical cyber systems in a timely manner using a risk-based methodology.

As noted above, in addition to developing and implementing a TSA-approved CIP, this directive requires the covered owner/operators to continually assess their cybersecurity posture. These owner/operators must develop and update a CAP and submit an annual plan to TSA that describes their program for the coming year, including details on the processes and techniques that they would be using to assess the

effectiveness of cybersecurity measures. Techniques such as penetration testing of IT systems and the use of "red" and "purple" team (adversarial perspective) testing are referenced in the SD. At a minimum, the CAP must include an architectural design review every 2 years. *See* section III.D.3. of this NPRM for additional discussion regarding the CAP required by the SD.

The scope of the requirements in this directive apply to Critical Cyber Systems. TSA defined a Critical Cyber System to include "any IT or OT system or data that, if compromised or exploited, could result in operational disruption. Critical Cyber Systems include business services that, if compromised or exploited, could result in operational disruption."[76]

On October 18, 2022, TSA issued an SD imposing similar performance-based cybersecurity requirements on higher-risk freight railroads and passenger rail owner/operators (SD 1580/82-2022-01).[77] This SD was also developed with extensive input from industry stakeholders and federal partners, including CISA and the FRA, to address issues unique to the rail industry. This engagement included providing the industry with a draft to review and comment upon and several meetings, including technical roundtables with cyber experts within the industry, before TSA issued the SD.

As TSA issued these directives under the statutory authority in 49 U.S.C. 114(*l*)(2) and intended the requirements to be in place for more than 90 days, TSA sought TSOB review and ratification of the use of the agency's emergency authorities. Table 2 provides the ratification dates for each SD.

TABLE 2: TSOB RATIFICATION DATES FOR TSA'S SDS

SD Series	Specific SD	Date of Ratification	Federal Register Citation
SD 1580-21-01	SD 1580-21-01	December 29, 2021	87 FR 31093 (May 23, 2022)
	SD 1580-21-01A	November 16, 2022	88 FR 36921 TBD (June 6, 2023)

[76] For purposes of this directive, "operational disruption" is defined as "a deviation from or interruption of business critical functions that results from a compromise or loss of data, system availability, system reliability, or control of a TSA-designated critical pipeline and rail system or facility." "Business critical functions" is defined as the "owner/operator's determination of capacity to support functions necessary to meet operational needs and supply-chain expectations.

[77] *See* https://www.tsa.gov/sites/default/files/sd-1580-82-2022-01.pdf (last accessed Oct. 19, 2022).

	SD 1580-21-01B	November 22, 2023	TBD
SD 1582-21-01	SD 1582-21-01	December 29, 2021	87 FR 31093 (May 23, 2022)
	SD 1582-21-01A	November 16, 2022	88 FR 36921 TBD (June 6, 2023)
	SD 1582-21-01B	November 22, 2023	TBD
SD 1580/82-2022-01	SD 1580/82-2022-01	November 16, 2022	88 FR 36921 (June 6, 2023)
	SD 1580/82-2022-01A	November 22, 2023	TBD
	SD 1580/82-2022-01B	Superseded[78]	N/A
	SD 1580/82-2022-1C	July 29, 2024	TBD
SD Pipeline-2021-01	SD Pipeline-2021-01	July 3, 2021	86 FR 38209 (July 20, 2021)
	SD Pipeline-2021-01A	December 29, 2021	87 FR 31093 (May 23, 2022)
	SD Pipeline-2021-01B	June 24, 2022	88 FR 36921 (June 6, 2023)
	SD Pipeline-2021-01C	June 21, 2023	89 FR 28570 (April 19, 2024)
	SD Pipeline-2021-01D	June 28, 2024	TBD
SD Pipeline-2021-02	SD Pipeline-2021-02	August 17, 2021	86 FR 52953 (Sept. 24, 2021)
	SD Pipeline-2021-02B	January 13, 2022	87 FR 31093 (May 23, 2022)
	SD Pipeline-2021-02C	August 19, 2022	88 FR 36921 (June 6, 2023)
	SD Pipeline-2021-02D	August 24, 2023	89 FR 28570 (April 19, 2024)
	SD Pipepilne-2021-02E	August 23, 2024	TBD

2. TSA's assessments, guidelines, and regulations applicable to pipeline and rail systems

The Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Act)[79] requires certain actions to enhance surface transportation security. The following two mandates are specifically relevant to this rulemaking.

a. Pipeline guidelines, assessments, and regulations

Section 1557(a) of the 9/11 Act requires a program to review pipeline operator adoption of guidelines originally issued by the DOT in 2002.[80] TSA originally reviewed operators' adoption of the Pipeline Security Information Circular, issued on September 5, 2002, by DOT's Office of Pipeline Safety as the primary federal guideline for industry security. TSA also reviewed operators' adoption of a complementary document, the DOT-issued Pipeline Security Contingency Planning Guidance of June 2002.

Recognizing that the Security Circular required updating, TSA initiated a process to amend the federal security guidance. These revised guidelines were first developed in 2010 and 2011 in collaboration with industry and government members of the Pipeline

[78] SD 1580/82-2022-01B, issued in May 2024, was superseded by SD 1580/82-2022-01C before ratification by the TSOB.
[79] Public Law 110-53, 121 Stat. 266 (Aug. 3, 2007).
[80] *Id.*, as codified at 6 U.S.C. 1207(a).

Sector and Government Coordinating Councils and other industry association representatives and included a range of recommended security measures covering all aspects of pipeline operations. Consistent with TSA's general authorities under ATSA and the requirements in section 1557(d) of the 9/11 Act, the advancement of security practices to meet the ever-changing threat environment in both the physical and cyber security realms required that the guidelines be updated again. Using a similar industry and government collaborative approach, TSA updated the Pipeline Security Guidelines in 2018 (Pipeline Guidelines).[81] As part of this update, TSA added Section 7, "Pipeline Cyber Asset Security Measures," including pipeline cyber asset identification; security measures for pipeline cyber assets; and cybersecurity planning and implementation guidance.

Section 1557(b) also requires reviewing the pipeline security plans and inspection of the most critical facilities for the 100 most critical pipeline operators.[82] The Pipeline Guidelines are used as the standard for TSA's Pipeline Security Program Corporate Security Reviews (CSRs) and Critical Facility Security Reviews (CFSRs) of the most critical pipeline systems. The CSR program has been in effect since 2003, during which time a total of approximately 260 CSRs have been completed industry wide. Approximately 800 CFSRs have been completed since this program's inception in 2009.

Finally, section 1557(d) specifically authorizes the Secretary of Homeland Security (Secretary) to issue regulations, as appropriate and following consultation with the Secretary of Transportation on the extent of risk and appropriate mitigation measures, and to issue binding regulations and carry out necessary inspection and enforcement actions.[83] Such regulations would incorporate the 2002 guidelines and contain additional

---

[81] *See* Pipeline Security Guidelines (Mar. 2018), with Change 1 (Apr. 2021), available at https://www.tsa.gov/sites/default/files/pipeline_security_guidelines.pdf (last accessed Sept. 19, 2022).
[82] *See* 6 U.S.C. 1207(b).
[83] *See* 6 U.S.C. 1207(d).

requirements as necessary based upon results of the inspections performed under section 1557(b). This section specifically authorizes assessment of penalties against pipeline facilities and systems for non-compliance.[84] While TSA has had this authority since 2007, TSA has not determined it was necessary to exercise it until this current rulemaking, which is intended to address the increasing cybersecurity threat to pipeline facilities and systems.

In addition, while the guidelines are available to all pipeline facilities and systems, regardless of whether TSA has determined the system is critical, TSA has not determined it is necessary to impose cybersecurity requirements through its emergency authorities on the full scope of pipeline owner/operators to which the guidelines are issued.

Although this rulemaking would impose cybersecurity requirements on certain pipeline owners and operators and subject such entities to inspections for compliance, TSA would continue to conduct voluntary security assessments in areas where mandatory requirements do not exist (*e.g.*, the physical security measures recommended in the guidelines) as part of a "structured oversight" approach. This approach assesses and provides feedback on voluntary implementation of cybersecurity recommendations for systems not covered by this proposed rule. These assessments would continue TSA's approach of working with the industry to determine the industry's voluntary adoption and adherence to non-regulatory guidelines, including Security Action Items and other security measures developed jointly with, and agreed to by, industry stakeholders to meet relevant security needs.[85] As part of these assessments, TSA provides recommendations to owner/operators and identifies resources to support them in voluntarily enhancing their physical and security baseline.

---

[84] *Id.* TSA also has specific authority to enforce its security regulations. *See* 49 U.S.C. 114(f)(7).
[85] For additional information on TSA's resources and surface transportation security initiatives, see TSA's website at: https://www.tsa.gov/for-industry/resources (last accessed Aug. 30, 2023).

b. Regulating railroads, public transportation systems, and OTRBs.

In 2008, TSA promulgated regulations imposing security requirements on owner/operators of freight railroads, rail transit systems, including passenger rail and commuter rail, heavy rail transit, light rail transit, automated guideway, cable car, inclined plane, funicular, and monorail systems. This regulation, in pertinent part, covers appointment of security coordinators and security-related reporting requirements. For freight railroads, the 2008 rule also imposed requirements for the secure transport of Rail Security-Sensitive Materials.[86]

In addition to measures to enhance pipeline security, the 9/11 Act required other regulations to enhance surface transportation security. On March 23, 2020, consistent with these requirements, TSA published the final rule, "Security Training for Surface Transportation Employees."[87] This regulation requires owner/operators of higher-risk freight railroad carriers (as defined in 49 CFR 1580.101), public transportation agencies (including rail mass transit and bus systems and passenger railroad carriers, as defined in 49 CFR 1582.101), and OTRB companies (as defined in 49 CFR 1584.101), to provide TSA-approved security training to employees performing security-sensitive functions. In addition to implementing these provisions, the final rule also expanded the requirement for security coordinators and reporting of significant security concerns to apply to OTRB and bus-only public transportation agencies, and defined Transportation Security-Sensitive Materials.[88]

The 9/11 Act also requires regulations for higher-risk public transportation agencies, railroads, and OTRB owner/operators to develop security plans to address specific security issues and vulnerabilities identified during an assessment of specific

---

[86] *See* Rail Transportation Security Final Rule (Rail Security Rule), 73 FR 72130 (Nov. 26, 2008).
[87] 85 FR 16456.
[88] *See* secs. 1512 and 1531 of the 9/11 Act, as codified at 6 U.S.C. 1162 and 1181, respectively, for security coordinator requirements. *See* sec. 1501(13) of the 9/11 Act, as codified at 6 U.S.C. 1151(13), for requirement to define "Transportation Security Sensitive Materials."

systems, infrastructure, and capabilities.[89] TSA published an advance notice of proposed rulemaking (ANPRM) in December 2016 seeking comment on specific issues related to the 9/11 Act's requirements for a regulation to address vulnerability assessments and security plans.[90] Through this ANPRM, TSA solicited information on the extent to which owner/operators of freight railroads, PTPR systems, and OTRBs had taken actions consistent with those prescribed by the 9/11 Act for vulnerability assessments and security plans, what resources they used to support these actions, and information on implementation costs. Given the passage of time and different scope of this rulemaking, TSA has established a new docket for this rulemaking and advises commenters on the 2016 ANPRM to submit comments on this NPRM if they wish for their views to be addressed in a final rule.

While the requirements in this proposed rule would not address all elements of vulnerability assessments and security plans stipulated in the 9/11 Act, it would address the 9/11 Act's requirements as they relate to the IT and OT systems used by high-risk freight railroads and PTPR systems. For example, the 9/11 Act requires identification and evaluation of critical systems, including information systems,[91] plans for providing redundant and backup systems needed to ensure continued operations in the event of a cybersecurity incident, and identification of the vulnerabilities to these systems.[92] The vulnerability assessment requirements applicable to higher-risk rail carriers must also identify strengths and weaknesses in (1) programmable electronic devices, computers, or other automated systems used in providing transportation; (2) alarms, cameras, and other protection systems; (3) communications systems and utilities needed for railroad security

---

[89] *See* secs. 1405 and 1512 of the 9/11 Act, as codified at 6 U.S.C. 1134 and 1162, respectively; *see also* section 1531, as codified at 6 U.S.C. 1181 (which imposes similar requirements for OTRBs).
[90] *See* 81 FR 91401 (Dec. 16, 2016).
[91] *See* secs. 1405(a)(3) and 1512(d)(1)(A) of the 9/11 Act, as codified at 6 U.S.C. 1134(a)(3), 1162(d)(1)(A), respectively.
[92] *See id.* at secs. 1405(c)(2), 1512(d)(1)(D), and 1512(e)(1)(G), as codified at 6 U.S.C. 1134(c)(2), 1162(d)(1)(D), 1162(e)(1)(G), respectively.

purposes, including dispatching and notification systems; and (4) other matters determined appropriate by the Secretary.[93] For security plans, the statute requires regulations that address, among other things, actions to mitigate identified vulnerabilities, the protection of passenger communication systems, emergency response, ensuring redundant and backup systems are in place to ensure continued operation of critical elements of the system in the event of a terrorist attack or other incident, and other actions or procedures as the Secretary determines are appropriate to address the security of the public transportation system or the security of railroad carriers, as appropriate.[94] The provisions proposed in this NPRM would satisfy such requirements as they relate to cybersecurity in high-risk public transportation agencies and railroads.

In short, the 9/11 Act provisions described above contain a combination of detailed requirements regarding vulnerability assessments and the content of security plans. Each of these provisions confirms and supplements TSA's authority to impose such requirements as are appropriate or necessary to ensure the security of the transportation system. TSA would issue the proposed rule pursuant to and consistent with its general authorities and the 9/11 Act's requirements.

C. References

1. National Cybersecurity Strategy

In March 2023, the Biden-Harris Administration released the National Cybersecurity Strategy.[95] This strategy includes the following five pillars identified as critical for building and enhancing the collaboration necessary to strengthen the nation's

---

[93] *See id.* at sec. 1512(d), as codified at 6 U.S.C. 1162(d).

[94] *See id.* at secs. 1405(c)(2) and 1512(e), as codified at 6 U.S.C. 1134(c)(2), 1162(e), respectively. Only one commenter on the ANPRM specifically addressed the inclusion of IT and OT systems for purposes of vulnerability assessments and security planning. *See* TSA-2016-0002-0013, available at https://www.regulations.gov under Docket No. TSA-2016-0002. This commenter indicated that, at the time of the comment, the Rail Information Security Committee of the Association of American Railroads focuses on cybersecurity and the "industry's physical and cyber security committees annually conduct risk assessments using "relevant security information" from a variety of resources. As part of this effort, they evaluate specific information technology and communication assets. They also indicated that the industry emphasizes analysis of cyber incidents and sharing information with railroads.

[95] *See supra* note 12.

cybersecurity posture to protect infrastructure critical to national security and the economy: (a) defend critical infrastructure; (b) disrupt and dismantle threat actors; (c) shape market forces to drive security and resilience; (d) invest in a resilient future; and (e) forge international partnership to pursued shared goals.

Consistent with this strategy, TSA is proposing a performance-based regulation for cybersecurity that builds on the NIST CSF and uses the CISA CPGs as guardrails to ensure prioritization of those measures most critical for establishing a common baseline to reduce known risks to national security and the economy.[96] The following provides a high-level overview of the NIST CSF and the CISA CPGs. A table that aligns these two documents with the proposed requirements in this NPRM is available in the docket for this rulemaking.

2. NIST Cybersecurity Framework

Executive Order (E.O.) 13636 of February 12, 2013 (Improving Critical Infrastructure Cybersecurity), directed NIST to develop a voluntary framework to reduce cyber risks to critical infrastructure.[97] This framework, created in collaboration between industry and government, consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The recommendations in the framework are intended to provide a prioritized, flexible, repeatable, and cost-effective approach to manage cybersecurity-related risks. The framework is not a regulatory document in that it is written as recommendations and is not enforceable. The recommendations are also extensive and may not be applicable to every business or context. NIST is currently in the process of reviewing and revising the Cybersecurity Framework. For purposes of this rulemaking, TSA has relied on Version 1.1 of April 16, 2018.

---

[96] *Id*. at 8-9.

[97] Published at 78 FR 11737 (Feb. 19, 2013). The Cybersecurity Enhancement Act of 2014, Public Law 113-274, 128 Stat. 2971, 2972-73, subsequently formalized the requirements in the E.O. into statutory requirements for NIST.

The NIST CSF is a comprehensive resource for developing a comprehensive cybersecurity program for any business. The framework generally includes the following key steps: (a) understanding the business's current cybersecurity posture by scoping the Organizational Profile; (b) gathering information needed to prepare the Organizational Profile, *i.e.*, defining a target state, which should be informed by standards and applicable regulations; (c) creating an Organizational Profile that identifies and prioritizes opportunities for improving within the context of continuous and repeatable processes; (d) analyzing the gaps between current state and the Target Profile, and creating an action plan to address any identified gaps, including a Plan of Action and Milestones; and (e) implementing the action plan and updating the Organizational Profile as necessary to keep the organization moving towards the target.[98] These steps are part of an iterative cycle that should also consider opportunities for documenting and communicating the organization's cybersecurity capabilities and known opportunities for improvement with external stakeholders, including business partners, prospective customers, suppliers, and other third parties.[99]

There are currently six core functions to the framework: govern, identify, protect, detect, respond, and recover. NIST recommends that all these functions be addressed concurrently as they all have vital roles related to cybersecurity.[100] Within each of these functions, there are multiple recommendations. Finally, the framework identifies several framework tiers in ascending order of cybersecurity maturity. The first and lowest tier, "Partial," recognizes an ad hoc, reactive, and irregular approach to cybersecurity that is driven by case-by-case responses in an environment that fails to identify clear roles and responsibilities for cybersecurity. The next tier, "Risk Informed," has a cybersecurity program that is approved by management but may not be known organization wide.

---

[98] *See supra* note 13 at 7.
[99] *Id.*
[100] *Id.* at 5.

While there may be an awareness of risk at certain levels within the organization, the company lacks an organization-wide process to manage risks and doesn't fully recognize both dependencies and dependents that could be affected by insufficient cybersecurity.

As companies mature in developing and implementing cybersecurity measures, they should be moving to a "Repeatable" tier. In this tier, processes are formally approved and are known and communicated organization wide. There is an organization-wide approach to managing risks, consistent methods are in place for cybersecurity policies, individuals within the company known their roles and responsibilities for cybersecurity, and the company is aware of dependencies and dependents. The top tier, "Adaptive," applies to companies that have implemented predictive, advanced technologies to address cybersecurity. In this tier, cybersecurity risks inform corporate decisions, and the company understands its role in the larger ecosystem and contributes to a broadening understanding of cybersecurity in its business environment. As part of this understanding, the company has a strong supply chain understanding and program to manage cybersecurity risks within the supply chain based on dependencies and dependents.

3. CISA Cross-Sector Cybersecurity Performance Goals

CISA developed the CPGs as directed by the National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems (signed July 28, 2021). The CISA CPGs can be read as a prioritized subset of the NIST CSF framework that critical infrastructure owners and operators can implement to meaningfully reduce the likelihood and impact of known risks and adversary techniques. As with the NIST CSF, the CISA CPGs are voluntary. Unlike the NIST CSF, the CISA CPGs are not intended to be comprehensive. Aligned with the NIST CSF, the CISA CPGs supplement that framework by supporting businesses in prioritizing cybersecurity measures critical for establishing a baseline of cybersecurity across critical infrastructure that emphasizes

measures based on their demonstrated ability to reduce known risks. The prioritization used in the CISA CPGs goes beyond consideration of risks to specific entities and considers the aggregate risk to the nation of cybersecurity incidents on critical sectors. The recommendations in the CISA CPGs align with the six core functions of the NIST CSF identified above.

4. TSA advance notice of proposed rulemaking

On November 30, 2022, TSA published an ANPRM to provide an opportunity for interested individuals and organizations, particularly higher-risk pipeline and rail (including freight, passenger, and transit rail) operations, to help TSA develop a comprehensive and forward-looking approach to surface cybersecurity requirements. The ANPRM also solicited input from the industry associations representing these companies, third-party cybersecurity subject matter experts, and insurers and underwriters for cybersecurity risks for these transportation sectors.[101]

TSA received comments from 35 commenters in response to the ANPRM, with almost 600 specific issues raised by the commenters, which included major trade associations and individuals.[102] Most comments received fell into a few general categories: (1) general support; (2) emphasis on the need for regulatory harmonization and performance-based regulation; and (3) comments on core elements, particularly comments related to training, supply chain, and third-party assessors. Some comments opposed potential regulation at this time, suggesting that voluntary measures are currently sufficient, and that TSA should wait for other standards (such as the CISA CPGs) to

---

[101] *See Enhancing Surface Cyber Risk Management,* 87 FR 73527 (Nov. 30, 2022). Through a subsequent notice, TSA extended the comment period from January 17, 2023, to February 1, 2023. *See* 87 FR 78911 (Dec. 23, 2022).

[102] Comments may be viewed in the docket for this rulemaking, TSA-2022-0001, at https://www.regulations.gov. The American Gas Association, American Fuel and Petrochemical Manufacturers, Association of American Railroads, American Short Line and Regional Railroad Association, American Public Transportation Association, Airlines for America, Liquid Energy Pipeline Association, Interstate Natural Gas Association, American Petroleum Institute, and AFL-CIO Transportation Trades Division were among the major trade associations that submitted comments.

further mature. TSA considered all comments received. The following provides a high-level summary of the comments.

a. General support and need for regulatory harmonization and performance-based regulation

The industry comments generally supported a regulation that builds upon the previously issued SDs. Many commenter groups complimented TSA's current performance-based directives, which provide owner/operators the flexibility to determine how to implement cybersecurity protocols to achieve the desired outcomes. Furthermore, they emphasized how adaptive CRM programming would enable regulated parties to—

- Assess known and potential system and environment vulnerabilities;
- Assess the likelihood and potential operational and financial impacts of a threat actor leveraging vulnerabilities to cause a cybersecurity incident;
- Develop a regular cadence of reassessing risk factors and recalculating risk; and
- Implement and monitor the effectiveness of appropriate mitigating controls to reduce the probability or impact of an attack.

A recurring theme in the ANPRM comments focused on encouraging TSA to use existing standards as a reference (*e.g.*, the NIST CSF, the CISA CPGs, and the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards[103]) and collaborate with other Federal agencies to harmonize cybersecurity requirements. Several respondents recommended that TSA facilitate a cross-government group composed of State and Federal agencies that would meet regularly (*e.g.*, monthly stakeholder calls or ongoing TSA-led briefings to relevant sector

[103] The NERC CIP standards are reliability standards for operators of the bulk electric system (BES). A small number of companies have both pipeline and BES business units. TSA is aware that when the agency transitioned from prescriptive security requirements in the first iteration of SD Pipeline-2021-02 to the performance-based requirements, some owner/operators subject to both the TSA and NERC requirements incorporated applicable measures into their implementation plans. TSA would continue to provide that flexibility with this proposed rule, to the extent that specific measures meet the performance standards identified in the proposed rule. TSA welcomes comments on any conflicts or divergences that TSA should take account of as part of this rulemaking.

coordinating officials) as well as develop common lexicons between these entities before issuing requirements.

b. Core elements

In the ANPRM, TSA sought comment on the following 11 core elements for a CRM program:

- Designation of an individual responsible for cybersecurity;
- Access controls;
- Vulnerability assessments;
- Penetration testing, drills, and exercises;
- Technical security controls;
- Physical security controls;
- Incident response planning & operational resilience;
- Incident reporting and information sharing;
- Personnel training & awareness;
- Supply chain/third-party risk management; and
- Recordkeeping and documentation.

While TSA reviewed all of the comments received, we also note that many of the comments reiterated issues raised in discussions with industry post-issuance of the SDs discussed above. The comments, however, also included three issues of particular interest to TSA as they applied to requirements included in this proposed rule that were not specifically in the SDs: employee cyber training, supply chain/third-party vendors, and third-party assessors.

c. Training

Many comments referenced or addressed workforce cyber training. Commenters acknowledged that security training is a critical component of overall organizational security and compliance. While generally supportive of the requirement, one of the

industry commenters recommended against establishing "specific training requirements," noting that specific training needs should be based on an organization's particular operating environment as well as the costs associated with a cybersecurity incident.

d. Supply Chain

The National Cybersecurity Strategy (March 2023) identifies the criticality of a secure global supply chain for information, communications, and OT products and services.[104] Consistent with this prioritization, DHS identified supply chain and third-party service provider risk management as a core element for DHS cybersecurity regulations. A majority of comments mentioned or addressed supply chain issues. Many commenters discussed their efforts to establish a common understanding with vendors and third parties through cybersecurity contract provisions regarding notifications of product vulnerability, access to security patches, notifications of cybersecurity incidents, etc. One association specifically noted that a number of pipeline operators are working with DHS to develop improved ways to facilitate conversations on security between vendors and operators.

e. Third-Party Assessors

The concept of third-party assessors was the topic of a significant number of comments. In general, commenters opposed requiring owners and operators to conduct assessments using third-party validators. Commenters considered such a requirement to be shifting costs from the government to the regulated parties. Companies within the different surface sub-sectors have varying degrees of capability and capacity to adopt cybersecurity standards. For example, one association indicated that they proactively conduct security control assessments of third parties and include them in response and recovery plans and exercises. Others, however, indicated they lack the capability and resources to use third-party assessors.

---

[104] *See* National Cybersecurity Strategy, *supra* note 12, at 32.

5. Regulatory Harmonization

As noted by the Office of the National Cyber Director (ONCD) in an August 2023 Request for Information, [105] the National Cybersecurity Strategy[106] calls for establishing cybersecurity regulations to secure critical infrastructure where existing measures are insufficient, harmonizing and streamlining new and existing regulations, and enabling regulated entities to afford to achieve security.

TSA emphasizes its commitment to regulatory harmonization and streamlining, and notes that this proposed rule, which is grounded in NIST's Framework for Improving Critical Infrastructure Cybersecurity, NIST's standards and best practices, and the CISA CPGs, is consistent with such priorities. TSA also acknowledges the ongoing rulemakings of other DHS components, including ongoing rulemakings on cybersecurity in maritime transportation and implementation of CIRCIA. Finally, TSA notes that this proposed rule follows several years of implementation of TSA's SDs. As noted in TSA's information collection requests for the SDs, TSA has not identified any other duplicative requirements for the cybersecurity mitigation measures required by the SDs and received no comments regarding duplication in response to notices published in the *Federal Register.*[107]

TSA's experience in imposing cybersecurity requirements to date, as well as feedback from the owner/operators subject to those requirements, indicates that complete harmonization is not possible. Even within the transportation sector, there are modal operational issues, different physical controls by other agencies that support defense-in-depth measures, as well as other factors that must be considered. For example, SD-

---

[105] *See* 88 FR 55694 (Aug. 16, 2023).
[106] *See supra* note 12.
[107] *See* OMB Approval No. 1652-0074 (Cybersecurity Measures for Surface Modes), approved through Aug. 31, 2026; and OMB Approval No. 1652-0056 (Pipeline Corporate Security Reviews and Security Directives), approved through Feb. 28, 2026; and OMB Approval No. 1652-0050 (Critical Facility Information of the Top 100 Most Critical Pipelines), approved through Mar. 31, 2026). One commenter noted that TSA's SDs require reporting within 24 hours while the CIRCIA proposed rule requires reporting within 72 hours. This issue is discussed *infra* in section III.D.2.f. of this proposed rule.

Pipeline-2021-02 recognizes that the need to provide ready access to industrial control workstations in controls rooms may make a requirement for multi-factor authentication (MFA) inadvisable. TSA allows owner/operators to rely on compensating controls use to meet control room requirements issued by the PHMSA.[108] Similarly, TSA provides an allowance for alternatives to encryption for certain systems used by railroads[109] and recognizes compliance with FRA's requirements to address access to PTC system components in locomotives.[110]

While TSA believes differences in cybersecurity requirements may be intentional based on sector-specific distinctions, TSA welcomes comments on opportunities to harmonize and streamline regulations where feasible and appropriate.

III. Proposed Rule

A. Rule organization

This rule proposes changes to the requirements applicable to owner/operators of freight railroads, PTPR, and OTRBs in subchapter D of title 49 CFR, subtitle B, chapter XII. The rule also proposes to add a new part 1586 to this subchapter, which would impose requirements applicable to owner/operators of specific pipeline facilities and systems.

To facilitate implementation of these requirements, TSA is proposing to significantly revise subchapter D. Some of these revisions are technical revisions to consolidate previously imposed procedures or requirements or to align procedures for security programs with TSA's existing processes for aviation. TSA believes consolidating procedural and general requirements in part 1570, while providing consolidated modal-specific requirements in modal-specific parts, would make it easier for owner/operators to identify and implement the proposed requirements. TSA is also

---

[108] *See* SD-Pipeline-2021-02 at Section III.C.2.
[109] *See* SD-1580/82-2022-01 at Section III.B.2.b.
[110] *See id.* at III.C.6.

proposing revisions to terms in part 1500 that have use in multiple provisions in chapter XII of title 49 and of part 1520 to ensure information required by the revisions to subchapter XII is protected as SSI, as applicable.

1. Cybersecurity requirements

The most significant proposed revision to TSA's regulations is the addition of requirements for higher-risk owner/operators of freight railroads, PTPR, and pipeline facilities and systems to have a comprehensive CRM program. These proposed requirements are found in new subpart D of part 1580 (applicable to freight railroads), subpart C of part 1582 (applicable to PTPR), and subpart C of part 1586 (applicable to pipeline facilities and systems). This proposed rule would also add a requirement in subpart B of part 1584 for higher-risk OTRB owner/operators to report cybersecurity incidents but would not impose the comprehensive CRM program requirements on this mode.

2. Physical security requirements

Through this rulemaking, TSA is proposing to distinguish between physical security and cybersecurity. TSA is proposing to move the requirements currently in subchapter D related to designating a security coordinator and reporting significant security concerns. TSA is proposing to move these requirements to revised subparts B within parts 1580, 1582, and 1584, respectively. These revised subparts B would contain security program requirements primarily focused on physical security. TSA also proposes to apply these same requirements to pipeline facilities and systems through the new part 1586. Appendix A to part 1570, which identifies types of significant security concerns to be reported, would be removed from part 1570 and repeated in parts 1580, 1582, 1584, and 1586.

As incorporated into this proposed subpart, TSA is proposing to clarify that the security coordinator(s) currently required by § 1570.201 must be a U.S. citizen. This

requirement is consistent with the 9/11 Act[111] and advances TSA's need to ensure that the agency can rapidly share sensitive information with the owner/operator that may be critical to ensure appropriate actions are taken to address emerging threats. As provided in the 9/11 Act, TSA may waive the citizenship requirement for the security coordinator(s) if the individual successfully completes a STA.[112]

In addition, the value of the security coordinator position is significantly impeded if there is not an individual in place who can receive sensitive information. Therefore, TSA is requiring that security coordinators (primary and alternate) must be a U.S. citizen who can receive sensitive information unless waived by TSA. At this time, TSA only anticipates one possible situation where a waiver would be granted; if one of the Security Coordinators is a U.S. citizen (primary or alternate), TSA may grant a waiver for the requirement as applied to the other Security Coordinator. From the agency's perspective, the purpose of the citizenship requirement is to ensure each covered owner/operator has a designated point of contact for receiving critical threat information, including intelligence information that cannot be shared with foreign citizens. TSA is assuming that owner/operators would ensure that if the security coordinator on duty is not cleared to receive certain information, that individual would promptly notify the security coordinator or other appropriate individual who has the required clearances. Both the primary and alternate Security Coordinators would be required to successfully complete an STA before TSA would consider a waiver.

TSA is also proposing to move any procedures or requirements applicable to training of security-sensitive employees[113] currently in 49 CFR 1570.101-1570.111, and 1570.121 to the applicable modal sections. Within the modal requirements, TSA is

---

[111] *See* secs 1512(e)(2) and 1531(e)(2) of the 9/11 Act, as codified at 6 U.S.C. 1162(e)(2) and 1181(e)(2), respectively.
[112] *Id.*
[113] *See* §§ 1580.3, 1582.3, and 1584.3 for definitions of "security-sensitive employees" as applied to freight railroads, PTPR, and OTRB, respectively.

proposing to consolidate the existing security training requirements into one section for each mode. None of the requirements would be changed as a result of this restructuring. Finally, the title of subpart C of part 1580, which includes chain of custody requirements applicable to the freight rail system, would be changed from "Operations" to "Security of Rail Security Sensitive Materials" without any revisions to the requirements in this subpart.

Physical security encompasses threats to physical infrastructure that could affect the safety and security of people, cargo, and infrastructure. The definition for physical security in this NPRM includes measures that provide for the security of systems and facilities, as well as the persons in areas in or near to operations that could have their safety and security threatened by an attack on physical systems and assets. Examples include rail cars, stations, pipelines, terminals, buses, *etc*. Cybersecurity is also critical for protecting the safety and security of people, cargo, and infrastructure, but the actions taken to prevent cybersecurity incidents are intended to protect computers, electronic communications systems and services, wire communications, and electronic communications, including information contained on these systems, services, and capabilities.[114]

It is important to recognize that there is not a bright line between physical and cybersecurity. A comprehensive defense-in-depth plan includes both physical and cybersecurity controls to protect IT and OT systems. For example, someone could use physical capabilities to damage an IT or OT system or thwart ineffective physical access controls to a building or floor in order to gain access to a Critical Cyber System. Similarly, physical security controls may be used to augment cybersecurity measures. Although TSA is distinguishing between Physical Security Coordinators and

[114] This explanation of cybersecurity is consistent with common understanding as reflected in the NIST Glossary, available at https://csrc.nist.gov/glossary/term/cybersecurity (last accessed July 6, 2023).

Cybersecurity Coordinators, we encourage these individuals to work together and communicate to ensure a comprehensive approach to both physical and cybersecurity.

3. General procedures for security programs, SDs, and Information Circulars

Through this rulemaking, TSA is also proposing to revise procedures in part 1570 related to security programs. When TSA promulgated the Security Training for Surface Transportation Employees final rule in 2020,[115] the rule text incorporated specific security program requirements. This structure reflected the limited scope of the requirements applicable to multiple modes of transportation. To accommodate the proposed addition of the cybersecurity requirements, TSA proposes to separate security training requirements, as discussed above, into the modal-specific parts and to incorporate general security program requirements that are consistent with the requirements applicable to aviation security programs. These changes, discussed in more detail in section III.F.1. of this preamble, would better ensure consistency across TSA's regulatory requirements. Table 3 provides a distribution table for these changes and those discussed above related to physical security requirements. TSA welcomes comment on the distribution table and whether any of the proposed changes might have unintended effects on existing requirements.

TABLE 3: 49 CFR CHAPTER XII, SUBCHAPTER D, DISTRIBUTION TABLE

Former Section	New Section
1570.107	1580.113(k), 1582.113(k), and 1584.113(k)
1570.109(b)	1580.113(h); 1582.113(h), and 1582.114(h)
1570.109(c)(1)	1570.107(a)(1)
1570.109(c)(2) and (3)	1570.107(a)(2)(i) and (ii)
1570.109(g)	1570.107(a)(2)(iii)
1570.111(a)	1580.113(i); 1582.113(i); and 1584.113(i)
1570.111(b)	1580.113(j); 1582.113(j), and 1584.113 (j)
1570.111(c)	1570.111
1570.113(b)(e)	1570.107(b)
1570.113(c) and (d)	1570.107 (amendment process); and 1580.113(o), 1582.113(o), and 1584.113(o) (physical security training specific requirements)
1570.113(f)	1570.107(b)
1570.113(g)	1570.107(f)

[115] *See supra* note 87.

1570.115(a)-(b).....	1570.107(d)
1570.115(c).....	1570.107 (e)
1570.117.....	1570.109 (narrow alternative process for seasonal or infrequent operations); 1570.203 (provides alternate measures for purposes of requirements in Security Directives)
1570.119.....	1570.107(f)
1570.121.....	1570.117 (general requirements); and 1580.113(l) and (m),1582.113(l) and (m), and 1584.113(l) and (m) (physical security training specific requirements)
1570.201.....	1580.103, 1582.103, and 1584.103
1570.203.....	1580.105. 1582.105, and 1584.105
Part 1570, appendix A.....	Part 1580, appendix C; part 1582, appendix C; and part 1584, appendix C
1580.101.....	1580.113(a)
1580.113(b)(1)-(5) and (7-9).....	1580.113(d)
1580.113(b)(6).....	1580.113(e)
1580.113(c).....	1580.113(g)
1580.115(a).....	1580.113(b)
1580.115(c).....	1580.113(c)
1580.115(c)-(f).....	1580.113(f)
1582.101.....	1582.113(a)
1582.113(b)(1)-(5) and (7-9).....	1582.113(d)
1582.113(b)(6).....	1582.113(e)
1582.113(c).....	1582.113(g)
1582.115(a).....	1582.113(b)
1582.115(c).....	1582.113(c)
1582.115(c)-(f).....	1582.113(f)
1584.113(b)(1)-(5) and (7-9).....	1584.113(d)
1584.113(b)(6).....	1584.113(e)
1584.113(c).....	1584.113(g)
1584.115(a).....	1584.113(b)
1584.115(c).....	1584.113(c)
1584.115(c)-(f).....	1584.113(f)

4. Relation to other rulemakings

TSA has other rulemakings that may reference subparts or sections contained in this proposed rule. Specifically, in the Vetting of Certain Transportation Employees NPRM, TSA has proposed to add vetting requirements as Subpart D of part 1580, Subpart C of part 1582, and Subpart C of part 1584.[116] In this rule, we are proposing to add CRM requirements in two of the same subparts, and are proposing to revise other provisions that are cross-referenced in the Vetting of Certain Surface Transportation Employees NPRM.[117] Although the substance of the two proposals do not conflict, the numbering and paragraph designations conflict in some cases. TSA will ensure all

[116] *See supra* note 17.
[117] *Id*.

subparts and sections are deconflicted and consistent before any rules are finalized.

B. Terms

1. General terms

Consistent with the proposed rule's organization, TSA includes proposed definitions for terms relevant to several subchapters of TSA regulations, beyond the requirements of subchapter D, in part 1500. Terms relevant to several parts of subchapter D would be added to § 1570.3. Terms uniquely relevant to each mode would be included in the relevant parts (part 1580 (freight), part 1582 (PTPR), part 1584 (OTRB), and part 1586 (pipeline facilities and systems)).

Most of the definitions are derived from existing federal regulatory programs, particularly programs administered by DOT. A few definitions are based on industry sources. TSA's purpose is to use definitions with which regulated parties are familiar, to the extent that the definitions are consistent with the purposes of this NPRM. Where no existing definition is appropriate, TSA's subject matter experts developed the definition based upon the generally accepted and known use of terms within each of the modes subject to this proposed regulation. Table 4 provides additional information on the terms that would be added to TSA's regulations.

TABLE 4: EXPLANATION OF PROPOSED TERMS AND DEFINITIONS IN SUBCHAPTER XII OF TITLE 49

Part	Summary of Change	Explanation
1500	Propose adding definition of "carbon dioxide"	This term is used in proposed sections regarding pipeline applicability in part 1586. Owner/operators of control rooms within this definition would, under certain criteria, be subject to the requirements in proposed part 1586. The proposed definition has the same meaning as the term is defined in in 49 CFR 195.2.
1500	Propose adding definition of "gas"	This term is used extensively in proposed part 1586 and refers to a commodity that, if transported by pipelines, may require the owner/operator to be subject to the requirements in part 1586. The term is also used in the definition of other terms defined in this proposed rule. The proposed definition aligns with the definition of this term in 49 CFR 192.3.
1500	Propose adding definition of "hazardous liquid"	This term is used extensively in proposed part 1586 and refers to a commodity that, if transported by pipelines, may require the owner/operator to be subject to the requirements in part 1586. The term is also used in the definition of other terms defined in this proposed rule. The proposed definition has the same meaning as the term is defined in in 49 CFR 195.2.
1500	Propose adding definition of "liquefied natural gas (LNG)"	This term is used extensively in proposed part 1586 and refers to a commodity that, if transported by pipelines, may require the owner/operator to be subject to the requirements in part 1586. The proposed definition has the same meaning as the term is defined in 49 CFR 193.2007.

1500	Propose adding definition of "pipeline or pipeline system"	This term is used extensively in proposed part 1586 and specifically refers to the means of transport of gas and hazardous liquids. Owner/operators of these systems would, under certain applicability criteria, be subject to the requirements in part 1586. The proposed definition has the same meaning as the term is defined in 49 CFR 192.3, 193.2007, and 195.2.
1500	Propose adding definition of "pipeline facility"	This term is used extensively in proposed part 1586 and specifically refers to the facilities used in the transportation of gas and hazardous liquids. Owner/operators of these systems would, under certain applicability criteria, be subject to the requirements in part 1586. The proposed definition has the same meaning as the term is defined in 49 CFR 192.3, 193.2007, and 195.2.
1500	Propose modifying definition of "transportation or transport"	TSA is proposing to update the definition to include the addition of pipeline system and facility operations to TSA's regulations through proposed part 1586.
1500	Propose modifying definition of "transportation facility"	This term is used in part 1520 and requirements (current and proposed) in subchapter D. TSA is proposing to update the definition to include pipeline system and facility operations in proposed part 1586.
1500	Propose modifying definition of "transportation security equipment and systems"	This term is used in part 1520 and requirements (current and proposed) in subchapter D of 49 CFR chapter XII. TSA is proposing to update the definition to include IT and OT authentication, network logging, and to specify that transportation security equipment and systems includes security equipment and systems for the protection and monitoring of both physical and virtual assets.
1500	Propose adding definition of "TSA Cybersecurity Lexicon"	This term would refer to a controlled vocabulary used in TSA's cybersecurity requirements. In general, the use of a standard lexicon reduces the possibility of misinterpretations when communicating cybersecurity definitions and terminology.
1570	Propose adding definition of "accountable executive"	This term is used in proposed sections regarding governance of a CRM program. Accountable executive means an individual employed by an owner/operator who is responsible and accountable for the owner/operator's compliance with the requirements of subchapter D, including authority over human resource issues, major financial issues, conduct of the owner/operator's affairs, all operations conducted related to the requirements of subchapter D, and responsibility for all transportation-related security issues.
1570	Propose adding definition of "cyber security-sensitive employee"	This term is used to describe employees of owner/operators who TSA proposes must receive cybersecurity-related training. The definition includes any employee who is a privileged user with access to, or privileges to access, a Critical Cyber System or any Information or Operational Technology system that is interdependent with a Critical Cyber System, as defined in the TSA Cybersecurity Lexicon.
1580	Propose adding definition of "defense connector railroad"	This term is used to identify applicability of CRM requirements and refers to a railroad that has a line of common carrier obligation designated a defense connector line by the US Army Military Surface Deployment and Distribution Command Transportation Engineering Agency (SDDCTEA) and the FRA, which connects defense installations or other activities requiring rail service to STRACNET.
1580	Propose adding definition of "switching or terminal services"	This term is used to identify applicability of CRM requirements and refers to persons primarily engaged in the furnishing of terminal facilities for rail passenger or freight traffic for line-haul service, and in the movement of railroad cars between terminal yards, industrial sidings and other local sites. *See* (https://www.osha.gov/sic-manual/4013)
1580	Propose adding definition of "train miles"	This term is used to identify applicability of CRM requirements. A Train-mile is the movement of a train (which can consist of many cars) the distance of one mile. A Train-mile differs from a vehicle-mile, which is the movement of one car (vehicle) the distance of one mile. A 10-car (vehicle) train traveling one mile would be measured as one Train-mile and 10 vehicle-miles. *See* (https://www.bts.gov/content/railroad-passenger-safety-data).
1582	Propose adding definition of "unlinked passenger trips"	This term is used in part 1582 and means the number of people making one-way trips on a public transportation system in a given time period.

1586	Propose adding definition of "control room"	This term is used in proposed sections regarding pipeline applicability in part 1586. Owner/operators of control rooms within this definition would, under certain criteria, be subject to the requirements in proposed part 1586. The proposed definition has the same meaning as the term is defined in 49 CFR 192.3 and 195.2.
1586	Propose adding definition of "high-consequence area"	This term is used in proposed part 1586 relating to the applicability of the requirements in that part. The proposed definition has the same meaning as the term is defined in 49 CFR 192.903 and 195.450.
1586	Propose adding definition of "peak shaving facility"	This term is used in proposed sections regarding pipeline applicability in part 1586. Owner/operators of peak shaving facilities would, under certain applicability criteria, be subject to the requirements in part 1586. There is no current federal definition of a "peak shaving facility," but the term has a commonly accepted interpretation across the industry.

2. TSA Cybersecurity Lexicon

TSA has also developed terms specific to cybersecurity requirements for purposes of its SDs and ICs discussed in section II.B.1. of this NPRM. Rather than including these terms in the regulation, TSA is proposing to add "TSA Cybersecurity Lexicon" to the terms in 49 CFR 1500.3. This term would refer to a controlled vocabulary used in TSA's cybersecurity requirements and be available on TSA's public website and any secure websites used to communicate with regulated entities. In general, the use of a standard lexicon reduces the possibility of misinterpretations when communicating cybersecurity definitions and terminology. The definitions provided below are generally consistent with those terms and definitions in the SDs and ICs.

As the meaning of cybersecurity terms can change over time based on emerging technology and capabilities, TSA is proposing to maintain these definitions separate from the regulatory text. Any changes to the terms would be interpretive in nature and would be made using the procedures for amendments to security programs described in proposed § 1570.107.

This approach also allows flexibility for TSA to align with other Federal agencies as part of broader effort to harmonize cybersecurity terminology and requirements without delaying the ability to proceed with this important rule to establish a strong cybersecurity baseline to protect critical surface operations. Table 5 includes the list and definition of terms that TSA proposes to establish for the first iteration of the TSA

Cybersecurity Lexicon.

TABLE 5: EXPLANATION OF PROPOSED TERMS AND DEFINITIONS IN TSA CYBERSECURITY LEXICON

Term	Proposed Definition	Explanation
Authorized representative	TSA is proposing to use a modified definition of an "authorized representative" from the definition in 49 CFR 1500.3. For TSA's cybersecurity requirements, an "authorized representative" is a person who is not a direct employee of the owner/operator but is authorized to act on the owner/operator's behalf to perform measures required by the security program. The term authorized representative includes agents, contractors, and subcontractors. This term does not include Managed Security Service Providers.	This term is used in proposed sections requiring, as necessary and appropriate, identification of individuals of third parties who are responsible for implementation or oversight of the CRM program of cyber activities identified or critical for implementation of cyber activities described in the owner/operators CRM program. Authorized representatives may be empowered to act on behalf of the authorizing official to coordinate and conduct the day-to-day activities associated with managing risk to information systems and organizations. Considering these responsibilities, authorized representatives may be liable for non-compliance separate or in addition to the owner/operator. [Source: NIST.SP.800-37r2]
Business critical functions	Owner/operator's determination of capacity or capabilities to support functions necessary to meet operational needs and supply chain expectations.	This term is used in proposed sections regarding Cybersecurity Incident Response Plans to determine key business functions, resources, infrastructure, and assets to ensure continuity of operations and supply chain expectations. [Source: Transportation Security Template and Assessment Review Toolkit]
Critical Cyber System	Any Information Technology or Operational Technology system used by the owner/operator that, if compromised or exploited, could result in an operational disruption incurred by the owner/operator. Critical Cyber Systems include those business support services that, if compromised or exploited, could result in operational disruption. This term includes systems whose ownership, operation, maintenance, or control is delegated wholly or in part to any other party.	This term is used in proposed sections to delineate criticality of any Information Technology or Operational Technology system to prioritize which assets need to be secured first. [Source: NIST IR 8179 / SD Pipeline-2021-02 series / SD 1580/82-2022-01 series]. These systems may include programmable electronic devices, computers, or other automated systems which are used in providing transportation; alarms, cameras, and other protection systems; and communication systems, and utilities needed for security purposes, including dispatching systems. [Source: sections 1531(d)(1)(C), 1512(d)(1)(C) of the Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. 110-53 (121 Stat. 266; Aug. 3, 2007)]
CISA	The Cybersecurity and Infrastructure Security Agency within the Department of Homeland Security.	This term is used in proposed sections related to reporting of cybersecurity incidents and protection of Critical Cyber Systems.
Cybersecurity Architecture Design Review	A technical assessment based on government and industry-recognized standards, guidelines, and best practices that evaluates systems, networks, and security services to determine if they are designed, built, and operated in a reliable and resilient manner. These reviews must be designed to be applicable to the owner/operator's Information Technology	This term is used in proposed sections to reflect an assessment for owner/operators in developing mitigation strategies to combat cyber intrusion and cybersecurity incidents. CISA offers an assessment called a Validated Architecture Design Review (VADR) while other third-party assessment entities offer a similar assessment based on CISA's VADR

	and Operational Technology systems.	methodology or a separate Architecture Design Review methodology. [Source: CISA Cyber Resource Hub / SD Pipeline-2021-02 series / SD 1580/82-2022-01 series]
Cybersecurity incident	An occurrence that, without lawful authority, jeopardizes or is reasonably likely to jeopardize the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident on the system. This definition includes an event that is under investigation or evaluation by the owner/operator as a possible cybersecurity incident without final determination of the event's root cause or nature (such as, malicious, suspicious, or benign).	This term is used in proposed sections to detail the elements of a cybersecurity incident in order to accomplish a harmonization of definition across the government. [Source: DHS Lexicon Ed 17 Rev 2 / SD Pipeline-2021-02 series / SD 1580/82-2022-01 series]
Information technology system	Any services, equipment, or interconnected systems or subsystems of equipment that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information that fall within the responsibility of an owner/operator subject to TSA's Cybersecurity Requirements to operate and/or maintain.	This term is used in proposed sections to describe what Information Technology system entails and align the definition with other Federal agencies. [Source: NIST SP 800-12r1 / CISA CPG / DHS Lexicon Ed 17 Rev 2 / SD Pipeline-2021-02 series / SD 1580/82-2022-01 series]
Interdependencies	Relationships of reliance within and among Information Technology and Operational Technology systems that must be maintained for those systems to operate and provide services.	This term is used in proposed sections to recognize the vital relationship between Information Technology and Operational Technology systems and used to determine the policies and controls that must be in place to secure critical cyber systems. [Source: SD Pipeline-2021-02 series / SD 1580/82-2022-01 series]
Least privilege	Persons and programs operate using the minimum level of access, permissions, and system resources necessary to perform the function.	This term is used in proposed sections to emphasize a security principle of granting minimum system resources and authorizations to accomplished assigned tasks. [Source: NIST SP 800-12r1/ SD Pipeline-2021-02 series / SD 1580/82-2022-01 series]
Managed Security Service Provider	For purposes of TSA's cybersecurity requirements, a person who is not a direct employee of the owner/operator, but who provides one or more services or capabilities that the owner/operator is using to perform measures required by the TSA. Managed Security Service Providers generally provide a logical service or capability. Managed Security Service Providers are not authorized representatives.	This term is used in proposed sections to make a distinction between a managed security service provider and an authorized representative for the purpose of identifying cybersecurity roles and responsibilities. [Source: NIST SP 800-61r2/ NIST SP 800-172 / Joint EA 23-01 Aviation]
Memorized secret authenticator	A type of authenticator comprised of a character string intended to be memorized by, or memorable to, the subscriber, permitting the subscriber to demonstrate something they know as part of an	This term is used in proposed sections to describe the makeup and function of a password and its critical role in the authentication process. [Source: NIST SP 800-63-3 / SD Pipeline-2021-02 series / SD

	authentication process.	1580/82-2022-01 series]
Operational disruption	A deviation from or interruption of business critical functions that results from a compromise or loss of data, system availability, system reliability, or control of systems.	This term is used in two contexts. First, it applies to identify reportable cybersecurity incidents. It is also used for purposes of identifying Critical Cyber Systems. The definition is intended to cover a wide range of potential scenarios. For example, while the term does not explicitly reference unauthorized access, presence of malicious software, or a distributed denial of service incident, those events are covered by the scenarios used in the definition. [Source: NIST SP 800-34r1 / SD Pipeline-2021-02 series / SD 1580/82-2022-01 series]
Operational technology system	A general term that encompasses several types of control systems, including industrial control systems, supervisory control and data acquisition systems, distributed control systems, and other control system configurations, such as programmable logic controllers, fire control systems, and physical access control systems, often found in the industrial sector and critical infrastructure. Such systems consist of combinations of programmable electrical, mechanical, hydraulic, pneumatic devices or systems that interact with the physical environment or manage devices that interact with the physical environment.	This term is used in proposed sections to describe what Operational Technology system encompasses and align the definition with other Federal agencies. [Source: NIST SP 800-37r2 / CISA CPG / SD Pipeline-2021-02 series / SD 1580/82-2022-01 series]
Phishing	Tricking individuals into disclosing sensitive information through deceptive computer-based means such as internet web sites or e-mails using social engineering or counterfeit identifying information.	This term is used in proposed sections to expound on a common cybersecurity incident that attempts to acquire sensitive data in which the perpetrator masquerades as a legitimate business or reputable person. [Source: NIST SP 800-150 / SD Pipeline-2021-02 series / SD 1580/82-2022-01 series]
Reportable cybersecurity incident	Incidents involving systems that the owner/operator has responsibility to operate and/or maintain including: a. Unauthorized access of an Information Technology or Operational Technology system; b. Discovery of malicious software that impacts the confidentiality, integrity, or availability of an Information Technology or Operational Technology system; c. Activity resulting in a denial of service to any Information Technology or Operational Technology system; and/or d. Any other cybersecurity incident that results in, or has the potential to result in, operational disruption affecting the owner/operator's Information Technology or Operational Technology systems; other aspects of the owner/operator's systems or facilities, critical infrastructure or core government functions; or national security, economic security, or public health and safety.	This term is used in proposed sections to inform the criteria for reporting when a cybersecurity incident occurs. [Source: TSA Surface IC/ SD Pipeline-2021-02 series / SD 1580/82-2022-01 series]
Security orchestration,	Capabilities that enable owner/operators to collect inputs monitored by the security	This term is used in proposed sections to highlight capabilities that enable

automation, and response (SOAR)	operations team. For example, alerts from the security information and event management system and other security technologies, where incident analysis and triage can be performed by leveraging a combination of human and machine power, help define, prioritize and drive standardized incident response activities. These capabilities allow an owner/operator to define incident analysis and response procedures in a digital workflow format.	owner/operators to monitor systems and drive standardized incident response. [Source: NIST SP 800-25 / SD Pipeline-2021-02 series / SD 1580/82-2022-01 series]
Shared account	An account that is used by multiple individuals with a common authenticator to access systems or data. A shared account is distinct from a group account, which is a collection of user accounts that allows administrators to group similar user accounts together in order to grant them the same rights and permissions. Group accounts do not have common authenticators.	This term is used to describe an account that required oversight/restriction due to unique requirement. [Source: NIST SP 800-53r5 (AC-2) / SD Pipeline-2021-02 series / SD 1580/82-2022-01 series]
Spam	Electronic junk mail or the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.	This term is used in proposed sections to describe unsolicited bulk emailed messages. [Source: NIST SP 800--12r1]
Tor, also known as The Onion Router	Software that allows users to browse the web anonymously by encrypting and routing requests through multiple relay layers or nodes. Tor software obfuscates a user's identity from anyone seeking to monitor online activity (such as nation states, surveillance organizations, information security tools). This deception is possible because the online activity of someone using Tor software appears to originate from the Internet Protocol address of a Tor exit node, as opposed to the address of the user's computer.	This term is used in proposed section to describe an open-source software for enabling anonymous internet communication. [Source: SD Pipeline-2021-02 series / SD 1580/82-2022-01 series]
Trust relationship	An agreed upon relationship between two or more system elements that is governed by criteria for secure interaction, behavior, and outcomes relative to the protection of assets. This term refers to trust relationships between system elements implemented by hardware, firmware, and software.	This term is used in proposed sections to recognize policies that govern how entities in differing domains honor each other's authorizations. [Source: NIST SP 800--160v1r1 / SD Pipeline-2021-02 series / SD 1580/82-2022-01 series]
Unauthorized access	Access from an unknown source; access by a third party or former employee; an employee accessing systems for which he or she is not authorized. This term may include a non-malicious policy violation such as the use of shared credential by an employee otherwise authorized to access it.	This term is used in proposed sections to describe what Unauthorized Access encompasses. [Source: SD Pipeline-2021-02 series / SD 1580/82-2022-01 series]

C. Cybersecurity Risk Management Program—General

1. Introduction

The primary purpose of this rulemaking is to mitigate the impacts of cybersecurity

incidents on higher-risk surface modes of transportation. This purpose will not be met by simply codifying the requirements in the SDs or assuming that what is currently being done will be sufficient for the future. Cybersecurity is not static; it is an ever-evolving capability to address ever-evolving threats. To ensure critical systems are protected from a cybersecurity incident, this proposed rule includes requirements to establish a CRM program that would ensure cybersecurity maturity as an ongoing and adaptive process.

In developing the requirements in this proposed rule, TSA began with those previously imposed by TSA through SDs issued under the authority of 49 U.S.C. 114(*l*), considered the structure and recommendations in the NIST CSF, and focused on the actions prioritized by CISA in the CPGs. Through implementation of these requirements, TSA believes the regulated parties would meet the NIST "Repeatable" Tier, which applies to companies with mature cybersecurity programs that are formally approved and are known and communicated organization-wide, reflect an organization-wide approach to managing risks, have consistent methods in place for cybersecurity policies, ensure individuals within the company know their roles and responsibilities for cybersecurity, and maintain an awareness of the company's dependencies and dependents.

2. Applicability

The applicability for this proposed rule is modified from the applicability of the current SD requirements. Specifically, the applicability of those SDs for railroads and rail transit systems generally aligns with the applicability for security training in 49 CFR part 1580 and 1582. For pipelines, applicability of the SDs aligns with TSA's designation of the most critical pipeline systems and facilities for purposes of the Pipeline Security Program Corporate Security Reviews and Critical Facility Security Reviews required by section 1557 of the 9/11 Act.[118] These applicability determinations were based on the physical security of transportation systems and risks within that context.

[118] *See supra* note 81.

Use of TSA's risk-based determinations for applicability is consistent with the focus of the 9/11 Act's requirements on higher-risk operations. This risk-based focus is reflected in the statutory requirement that focuses security training requirements on frontline employees, not all employees;[119] requiring risk-based tiers where only the highest tier would be required to comply with regulations for vulnerability assessments and security plans;[120] and focusing the pipeline security reviews on the most critical systems and facilities.[121] To expedite use of TSA's emergency authorities under 49 U.S.C. 114(*l*)(2), the agency primarily relied on the risk determinations used for these requirements and reviews to impose the cybersecurity requirements in the SDs discussed in section II.B.1 of this NPRM.

Since issuance of these SDs, TSA has determined that with respect to permanent regulations, different risk criteria apply when the focus is on cybersecurity. In addition to protecting passengers and the immediate supply chain, risk considerations also include protecting national security, including economic security, and recognizing their dependence on reliable freight rail and pipeline systems. As risk is a construct of threat, vulnerabilities, and consequences, the change from physical to virtual risks involves different types of threats related to motivation and capacity, different vulnerabilities reflecting reliance on IT and OT systems and dependency, and different consequences to passenger safety and the supply chain if a Critical Cyber System is the target of a successful cybersecurity incident. Where cybersecurity incidents in some sectors are primarily focused on loss of data or privacy information, in the transportation sector, a cybersecurity incident has a potential impact on operations affecting passenger safety, the environment, and the supply chain. In other words, cybersecurity incidents could have

---

[119] *See* secs. 1408(a), 1517(a), and 1534(a) of the 9/11 Act, codified at 6 U.S.C. 1137(a), 1167(a), and 1184(a), respectively.
[120] *See* secs. 1512(a) and 1181(a) of the 9/11 Act, codified at 6 U.S.C. 1162(a) and 1181(a).
[121] *See supra* note 81.

direct physical consequences. *See* discussion in section II.A.4. regarding cybersecurity threats. As noted in the National Cybersecurity Strategy, regulatory agencies are encouraged to ensure "cybersecurity regulations for critical infrastructure . . . prioritize the availability of essential services."[122] The expanding nature of cyber risks to the transportation sector also requires an assessment of applicability specific to these risks.

Consistent with these considerations, TSA is proposing the following applicability criteria for freight railroads, rail transit and passenger railroads, and pipelines facilities and systems.

a. Freight railroads subject to CRM program requirements in proposed subpart D of part 1580

TSA proposes that the CRM program requirements apply to the freight railroads that transport the greatest amount of cargo or are identified as supporting certain Department of Defense (DoD) operations. TSA estimates 73 freight railroads would meet the following risk-based criteria:

- Is a Class I railroad as defined in current 49 CFR 1580.3;[123] or
- Is a Class II or III railroad that:
  - Transports one or more of the categories and quantities of Rail Security-Sensitive Materials[124] in a High Threat Urban Area;[125]
  - Provides switching or terminal services to two or more Class I railroads;
  - Operates an average of at least 400,000 train miles in any of the three

---

[122] *See supra* note 12, at 8-9.
[123] TSA currently defines a Class I railroad by reference to the classifications of the Surface Transportation Board. For regulatory purposes, the Surface Transportation Board categorizes rail carriers into three classes: Class I, Class II, and Class III. The classes are based on the carrier's annual operating revenues. Current thresholds establish Class I carriers as any carrier earning revenue greater than $943.9 million, Class II carriers as those earning revenue between $42.4 million and $943.9 million, and Class III carriers as those earning revenue less than $42.4 million. *See* 49 CFR part 1201; General Instructions 1-1. TSA is proposing to revise its definition applicable to class determinations to include Class I, Class II, and Class III freight railroads.
[124] 49 CFR 1580.3.
[125] Appendix A to 49 CFR part 1580.

years before the effective date of the final rule or in any calendar year after the effective date;[126]

- Is designated as a Defense Connector Railroad by DoD, as defined in proposed 1580.3; or
- Serves as a host railroad to any of the freight railroad operations identified above or a higher-risk passenger rail operation identified in proposed § 1582.201;[127]

This criteria for applicability would capture railroads responsible for approximately 94 percent of the freight transported by rail in the United States, railroads that transport the largest volume of cargo, and railroads that serve as critical connections between Class I railroads or serve as vital links in the Strategic Rail Corridor Network (STRACNET).[128] A cybersecurity incident affecting one of these railroads would have the most significant impact on rail transportation, national security, and economic security.

The proposed applicability criteria for CRM program requirements would expand the applicability of the requirements set forth in the SDs to include an additional nine railroads, all of which operate more than an average 400,000 train miles[129] per year. TSA is proposing this expansion because these railroads represent a population that, were they to experience a degradation of service due to a cybersecurity incident, the effects of that service-degradation would ripple across the nation's rail network and cause significant disruption to the industry's service capacity.

---

[126] TSA reviewed historical statistics from the FRA to discern a threshold of annual train miles. The 400,000 train-miles threshold provided a clear breakpoint between large, medium, and small railroad operations. *See* https://railroads.dot.gov/accident-and-incident-reporting/overview-reports/train-miles-and-passengers (last accessed Sept. 27, 2023).

[127] 49 CFR 1582.101.

[128] The Strategic Rail Corridor Network is an interconnected and continuous rail line network consisting of over 36,000 miles of track serving over 120 defense installations.

[129] A train-mile is a unit in railroad accounting and refers to the distance of one mile covered by a single train, which may have several cars.

TSA is not proposing to apply the CRM program requirements to most short line and regional railroads. Although TSA's current regulations in 49 CFR part 1580 apply some requirements to the majority of the Short Line and regional railroads, these are not generally high-cost requirements. Applying the CRM program requirements to these smaller railroads would, however, impose costs with limited corresponding benefits to minimize the consequences that the proposed rule is intended to address as there would not be a significant impact on national security, including economic security, if one of these railroads had operational disruption due to a cybersecurity incident. An expanded scope of applicability could also be beyond TSA's current resources to effectively monitor for compliance. For those operators not determined to be at higher-risk, TSA believes it is more beneficial to continue issuing recommendations and engagements through field inspector outreach, trade association webinars, and other events to encourage railroad owner/operators not subject to TSA's requirements to take voluntary preventive measures to enhance their cyber security.

TSA is not proposing to include rail hazardous materials shippers and receivers in the scope of applicability for CRM requirements. TSA regulates these entities for purposes of "chain of custody" requirements in subpart C of 49 CFR 1580 due to their role at the beginning and end of the line for transporting Rail Security Sensitive Materials (RSSM). Based on their position in the supply chain, the security of these materials necessitates that these entities receive and share critical security information. To meet this need, TSA requires shippers and receivers of RSSM to have Physical Security Coordinators and to report physical incidents affecting these operations that could have an impact on the security of the shipment during transport by a freight railroad. We do not regulate operations within these facilities and do not intend to expand the scope of our requirements through this proposed rule.

Finally, TSA currently requires all freight railroads to have a security coordinator

and report significant security concerns focused on physical security.[130] Similarly, TSA is proposing that all freight railroads currently required to have a security coordinator and report significant security concerns, also have designated individual(s) responsible to serve as a Physical Security Coordinator and/or a Cybersecurity Coordinator[131] and report significant physical security concerns to TSA and cybersecurity incidents to CISA. Although the costs of a robust CRM program for the broader scope of freight railroads may not be justified at this time based on known risks, that determination does not mean that cybersecurity should be ignored. All railroads need a point of contact for receiving and processing information on cybersecurity risks, and the U.S. government needs to be promptly advised of any cybersecurity incidents involving these railroads to have a thorough understanding of the current threat environment.

b. Public transportation agencies and passenger railroads subject to CRM program requirements in proposed subpart C of part 1582

The criteria for applicability of the CRM program requirements for PTPR systems consider both location and passenger volume as primary risk considerations. Based on these considerations, TSA is proposing that the CRM rule apply to those rail transit systems and passenger railroads with the largest daily ridership. A successful cybersecurity incident against one or more of these systems or railroads could have a significant impact on the transportation sector, with consequences to national and economic security.

TSA estimates that 34 rail transit and passenger railroads, including Amtrak, would meet the following risk-based criteria:

- Is Amtrak (also known as the National Railroad Passenger Corporation) or

---

[130] *See* current 49 CFR 1570.201 and 1570.203.

[131] TSA is not preventing an owner/operator from designating the same individual(s) to serve as the Physical Security Coordinator and Cybersecurity Coordinator (or alternate) if all of the applicable requirements are met. At the same time, TSA recognizes that some owner/operators may want to have different individuals serve in these functions based upon their individual expertise and understanding of operations.

other a passenger railroad with average daily unlinked passenger trips of 5,000 or greater in any of the three previous years before the effective date of the final rule, or within any single calendar year after the effective date; Is a passenger railroad that hosts a Class I railroad or Amtrak, regardless of ridership volume; or

- Is a rail transit system with average daily unlinked passenger trips of 50,000 or more per year in any of the three calendar years before the effective date of the final rule, or any single calendar year after the effective date of the final rule.

TSA is proposing to define "unlinked passenger trips" in § 1582.3 as the number of times an individual boards public transportation as counted each time a vehicle is boarded, not based on travel from origin to destination. For example, a person riding only one vehicle from origin to destination takes one unlinked trip. A person who transfers to a second vehicle while travelling from origin to destination takes two unlinked trips. In some contexts, "unlinked passenger trips" are also referred to as "boardings." For purposes of this proposed rule, however, TSA is consistently using "unlinked passenger trips."

This scope of applicability would limit the economic burden to the highest consequence operators while still accounting for greater than 90 percent of the total nationwide daily rail ridership volume.[132] Consistent with the 9/11 Act, each of the systems that would be required to develop and implement a CRM program is eligible to receive grant funding under section 1406 of the 9/11 Act, 6 U.S.C. 1135, and has received such funding. Transit bus and smaller transit rail and passenger rail systems would not be included in the applicability of the CRM components of this proposed

[132] TSA's proposed applicability reflects analysis of ridership data developed by the APTA. *See* https://www.apta.com/research-technical-resources/transit-statistics/ridership-report/ridership-report-archives/ (last accessed Sept. 27, 2023).

rulemaking as the smaller ridership of these systems means the operational disruption would not have the same consequences as impacts on larger operations. If one of these systems is taken offline due to a cybersecurity incident, it would be temporarily disruptive, but would be unlikely to have significant impacts on national or economic security, compared to the disruption of the transit system in a major metropolitan area where public transportation is relied on by many commuters. Similarly, transit bus plays a pivotal role in the movement of people in urban areas, but TSA assesses that a cybersecurity incident affecting this mode of transportation is unlikely to result in a significant operational disruption because transit bus systems do not rely heavily on OT systems and likely could continue to operate in the event of a cybersecurity incident. The proposed applicability for this rulemaking does not include the following four systems that currently fall under the security training requirements in part 1582: Connecticut Department of Transportation (Conn DOT), Delaware River Port Authority, Santa Clara Valley Transportation Authority, and Staten Island Railway. These systems are not included because they did not meet the proposed risk-based criteria, *i.e.,* ridership threshold, determined by TSA as relevant to the specific risks this rulemaking is intended to address.

Although not subject to all of the CRM program requirements, TSA is proposing that all PTPR owner/operators currently required to have a security coordinator and report significant security concerns, also have designated individual(s) responsible to serve as a Physical Security Coordinator and/or Cybersecurity Coordinator and report significant physical security concerns to TSA and cybersecurity incidents to CISA.[133] The costs of a robust CRM program may not be justified at this time based on known risks, but that determination does not mean that cybersecurity should be ignored. All PTPR owner/operators need a point of contact for receiving and processing information

[133] *See* text accompanying *supra* note 131.

on cybersecurity risks, and the U.S. government needs to be promptly advised of any cybersecurity incidents involving these systems to have a thorough understanding of the current threat environment.

c. OTRB owner/operators subject to cybersecurity incident reporting requirements in proposed § 1584.107

TSA is not proposing that OTRB owner/operators be required to meet all CRM program requirements, but believes it is appropriate for those OTRB owner/operators required to report significant security concerns[134] be required to report both significant physical security concerns and cybersecurity incidents. TSA estimates that 71 OTRB owner/operators would be subject to this requirement.

Through this rulemaking, TSA is proposing to codify and make permanent the cybersecurity requirements previously imposed through SDs issued to address an immediate threat to transportation security. *See* discussion in section II.B. of this NPRM. TSA has not imposed cybersecurity mitigation measures on OTRB owner/operators based on the risk information currently available to the agency and recognition of the costs as related to the benefits. That decision, however, does not mean that there is zero risk for OTRB operations and that they will never be the victim of a cybersecurity incident. TSA has encouraged OTRB owner/operators to identify Cybersecurity Coordinators, report cybersecurity incidents, have a cybersecurity incident response plan, and conduct a vulnerability assessment.[135] TSA believes that higher-risk OTRB owner/operators should be vigilant regarding cybersecurity risks and is proposing that the U.S. government be promptly advised of any cybersecurity incidents involving these owner/operators in order to have a thorough understanding of the current threat environment. Requiring this information is consistent with TSA's authority to assess

---

[134] 49 CFR 1570.203.

[135] *See* Information Circular (IC)-2021-01 (effective Dec. 31, 2021), available at https://www.tsa.gov/sites/default/files/20211201_surface-ic-2021-01.pdf (last accessed Sept. 21, 2023).

threats, share information, and develop policy.[136]

TSA notes that the 9/11 Act requires TSA to issue regulations to higher-risk OTRB owner/operators to conduct vulnerability assessments and implement TSA-approved security plans that address the security of IT and OT systems.[137] TSA has not yet issued such regulations, although it has issued ICs recommending voluntary implementation of specific cybersecurity measures to higher-risk OTRB owner-operators.[138] TSA will consider reports of both significant physical security concerns (as required by current § 1570.201 and proposed § 1584.105) and cybersecurity incidents as reported under proposed § 1584.107 for purposes of developing future regulatory requirements.

d. Pipeline systems and facilities subject to physical security requirements in proposed subpart B of part 1586 and CRM program requirements in proposed subpart C of part 1586

TSA is proposing to apply the CRM program requirements to the hazardous liquid, natural gas, and liquefied natural gas pipeline systems and facilities that transport the largest volume of these commodities, which would lead to the potential for a sustained disruption in service should a successful cybersecurity incident affect their ability to support national security needs, including economic security. The recommended criteria for determining applicability of the requirements includes three types of pipeline operations: (1) hazardous liquid pipelines; (2) natural and other gas pipelines; and (3) liquefied natural gas (LNG) facilities. In total, the proposed requirements would apply to 115 owner/operators of covered pipeline facilities and

---

[136] *See, e.g.*, 49 U.S.C. 114(f)(1)-(3) (authority to receive, assess, and distribute intelligence information related to transportation security; assess threats to transportation; and develop policies, strategies, and plans for dealing with threats to transportation security).

[137] *See supra* section II.B.2.b of this NPRM.

[138] *See* Surface-IC-2021-01, Enhancing Surface Transportation Cybersecurity (Dec. 31, 2021), available at https://www.tsa.gov/sites/default/files/20211201_surface-ic-2021-01.pdf (last accessed Sept. 27, 2023); *see also* information regarding resources and activities supporting security of highway and motor carriers available on TSA's website at https://www.tsa.gov/for-industry/resources (last accessed Sept. 27, 2023).

systems.

First, TSA is proposing to apply the CRM program requirements to owner/operators of hazardous liquid or carbon dioxide pipeline facilities and systems that meet any of the following criteria:

- Owns or operates a hazardous liquid pipeline or facility subject to 49 CFR part 195 that—
  - Annually delivered hazardous liquids in excess of 50 million barrels in any of the three calendar years before the effective date of the final rule, or any single calendar year after the effective date of the final rule; or
  - Is in excess of 200 segment miles of pipeline transporting hazardous liquid or carbon dioxide that could affect a High Consequence Area, as defined by PHMSA.[139]
- Owns or operates a primary control room responsible for multiple hazardous liquid or carbon dioxide systems regulated under 49 CFR part 196 and the total annual delivery for those systems combined is greater than 50 million barrels annually in any of the three calendar years before the effective date of the final rule, or any single calendar year after the effective date of the final rule.
- Owns or operates a hazardous liquid pipeline or facility subject to 49 CFR part 195 that has a contract with the Defense Logistics Agency to supply hazardous liquids in excess of 70,000 barrels annually.[140]

Based on pipeline systems and facilities that report annual throughput to the Federal

[139] *See* proposed 49 CFR part 1586 for a definition of High Consequence Area and a discussion of Terms in subsection D of this section.
[140] TSA coordinated the criteria for 70,000 barrels with the Defense Logistics Agency. This amount conforms to what TSA uses to identify critical pipeline systems ("Top 100").

Energy Regulatory Commission (FERC),[141] TSA estimates these systems and facilities account for approximately 90 percent of the total annual volume transported in the United States.

Second, TSA is proposing to apply the CRM program requirements to owner/operators of natural gas and other gas pipelines that meet any of the following criteria:

- Owns or operates a natural or other gas system subject to 49 CFR part 192 and—
  - Annually delivered natural or other gas in excess of 275 million dekatherms annually (generally natural gas transmission) in any of the three calendar years before the effective date of the final rule, or any single calendar year after the effective date of the final rule;
  - Annually delivered natural or other gas to 275,000 or more meters (or service points) annually (generally natural gas distribution or local distribution company (LDC)) in any of the three calendar years before the effective date of the final rule, or any single calendar year after the effective date of the final rule; or
  - Has more than 200 segment miles that could affect a High Consequence Area.
- Owns or operates a primary control room responsible for multiple natural gas and other gas pipeline systems regulated under 49 CFR part 192 and the combined total annual delivery for these systems is greater than 275 million dekatherms (generally natural gas transmission) in any of the three calendar years before the effective date of the final rule, or any single calendar year

[141] Hazardous Liquid Pipeline Operators subject to FERC jurisdiction provide annual throughput (number of barrels delivers out) to FERC on Form 6, *Annual Report of Oil Pipeline Companies.*

after the effective date of the final rule.

- Provides natural or other gas service to 275,000 or more meters (or service points) annually (generally natural gas distribution or LDC) in any of the three calendar years before the effective date of the final rule, or any single calendar year after the effective date of the final rule.

TSA estimates that under these criteria, the requirements of this proposed rule would be applicable to an estimated 66 natural gas transmission and distribution pipeline systems and facilities. These systems and facilities account for approximately 80-90 percent of the total annual volume of natural gas transported in the United States.[142]

Third, TSA is proposing to apply the CRM program requirements to LNG facilities that import natural gas or operate as peak-shaving facilities.[143] Under the proposed criteria, the requirements would apply to an estimated two LNG import facilities and seven peak-shaving facilities. Expanding applicability of the proposed rule from the initial SDs for pipeline facilities and systems to include these facilities reflects TSA's ongoing discussions with FERC and evolving understanding of cybersecurity risks. The inclusion of these criteria would not significantly affect the number of pipeline systems and facilities subject to the CRM program requirements as all but one of the covered LNG facilities are operated by pipeline companies subject to the other criteria.

The SDs issued to pipeline owner/operators used criteria to include all hazardous liquid and natural gas pipeline systems and facilities that had been designated critical by TSA for purposes of the assessments required by the 9/11 Act. The scope of applicability, however, only accounts for approximately 10 percent of the total number of pipeline systems in the United States. At the other end of the spectrum for the possible

---

[142] TSA's data is derived from the Pipeline and Gas Journal's Annual 500 Report. For more information on this report, *see* https://pgjonline.com/magazine/2022/november-2022-vol-249-no-11/features/annual-500-report-shows-some-decline-few-ranking-surprises (last accessed Sept. 27, 2023).

[143] Peak-shaving refers to LNG facilities supplying supplemental gas supplies to meet the increased demand for natural gas on the coldest days of winter. In 2022, two plants located in the Northeast United States imported LNG.

scope of applicability, TSA determined it would not be appropriate to recommend covering all pipeline operators subject to PHMSA's safety regulations in 49 CFR part 192 and 49 CFR 195.1. This option, which includes approximately 2,105 pipelines, would be unnecessarily expensive for the industry based on the expected benefits and extremely difficult for TSA to appropriately monitor and regulate without additional personnel and funding. The proposed criteria for determining applicability would include the most critical pipeline owner/operators as determined by TSA and is consistent with the statutory requirement to determine critical operators[144] as well as TSA's designation of critical owner/operators required to comply with TSA's SDs.

e. Determinations of applicability for requirements in the proposed rule

As with TSA's previously issued requirements for surface transportation owner/operators,[145] owner/operators would be required to use the criteria in 49 CFR parts 1580, 1582, 1584, and 1586 to determine whether their operations are higher-risk and which requirements apply to them. Under § 1570.105(a), owner/operators would be required to notify TSA within 30 days of the effective date of the final rule if they meet the criteria for applicability of the requirements in the rule. TSA also proposes an obligation for owner/operators to be aware of the criteria as applied to their future operations. Under section 1570.105(b), TSA would continue to require owner/operators to notify TSA if their operations change, after the notification date specified in paragraph (a), such that the criteria apply. In this situation, an owner/operator would be required to notify TSA no more than the later of (a) 60-days after the effective date or (b) 60-days before commencing the new operations.

This notification requirement is the first compliance deadline that owner/operators

---

[144] 9/11 Act sec. 1557, as codified at 6 U.S.C. 1207(b).
[145] *See* current 49 CFR 1570.105.

must meet under the proposed rule. TSA is aware that the deadlines could cause confusion and concern among owner/operators who are currently required to comply with requirements issued by TSA, such as those issued in 2008[146] and 2021,[147] that are also in parts 1580, 1582, 1584, and 1586. To avoid any confusion over whether notification is required, TSA is proposing to add to § 1570.105(a) an exception that effectively exempts the owner/operator from this requirement if TSA has otherwise notified the owner/operator that the criteria apply. If this notification is received, these owner/operators would not need to provide separate notification regarding applicability determinations.

To mitigate the likelihood of an owner/operator failing to comply based upon lack of recognition of the applicability for these requirements, TSA also intends to use a variety of communication strategies to notify regulated parties that are likely to meet the applicability criteria. For example, TSA would use e-mail to immediately notify its key stakeholder points of contact regarding publication of a final rule. In addition to these established information sharing mechanisms, TSA also conducts regular calls, workshops, and meetings with major industry partners and trade associations. TSA's surface representatives also work closely with surface-system owner/operators during industry-led security work groups, conferences, roundtables, and other sector-specific government coordination meetings. TSA would use all these mechanisms to notify relevant industry partners of the new requirements.

TSA is also proposing to modify § 1570.105 to add paragraph (c), which would make it clear that once an owner/operator meets the criteria for applicability, they must continue to comply with the requirements in the proposed rule. New paragraph (d) provides an avenue for owner/operators to request to be removed from the scope of

---

[146] *See supra* note 86.
[147] *See supra* note 87.

applicability. For example, if an owner/operator meets the applicability criteria because of a contract to support STRACNET, but a future change removes them from that role, they would continue to be subject to the requirements until they notify TSA of the changed circumstances and receive a written determination from TSA that they are currently exempt from the requirements. TSA is not imposing a specific timeline for making this notification as it would be within the discretion of the individual owner/operator to seek an exemption. As noted above, the owner/operator would continue to be subject to the requirements until TSA makes a final decision that the owner/operator, or a specific activity of the owner/operator, no longer meets the applicability criteria.

It is the owner/operator's responsibility to notify TSA, in writing, that their operations have changed and to provide supporting documentation. TSA may also need to request additional documentation to support the assertion that the requirements no longer apply. For example, documentation may include proof that contracts with DoD have been rescinded or that they have been operating 30 percent below the threshold for applicability for three consecutive years. This provision should not be used for non-permanent changes. For example, an owner/operator may have seasonal operations two-months of every year that meet the criteria for applicability. In this situation, the owner/operator should seek alternative measures under proposed § 1570.109.

An exemption from TSA under § 1570.105(c) is operation specific. If operations change in the future such that they meet the criteria for applicability, the owner/operator would be required to comply with § 1570.105(a) and notify TSA. This notification must be provided within 90 days before commencement of operations that would meet the criteria for applicability of requirements in parts 1580, 1582, 1584, or 1586.

3. Structure of CRM program requirements (proposed §§ 1580.303, 1582.203, and 1586.203)

This proposed rule requires a CRM program that includes three major components: (a) a cybersecurity evaluation; (b) a COIP; and (c) a CAP. First, the cybersecurity evaluation generally aligns with the assessments required by TSA in the SD Pipeline-2021-01, SD 1580-21-01, and SD 1582-21-01 series. This evaluation is also consistent with the NIST CSF, which recommends that a strong cybersecurity program begins with an understanding of the current profile of cybersecurity that looks at both physical and logical/virtual controls.

Second, owner/operators would be required to develop and implement a TSA-approved COIP. This plan aligns with the requirements for a CIP required by the SD Pipeline-2021-02 and SD 1580/82-2022-01 series. As with the CIP requirements in the SDs, the COIP requirements generally apply to Critical Cyber Systems as identified by the owner/operators. TSA is proposing to incorporate other parts of the SDs, including the Cybersecurity Coordinator, requirement to report cybersecurity incidents, and the CIRP, into the COIP.

The COIP requirements, which are organized in to align with the NIST components, focus on the following five areas: (1) governance of the CRM program, (2) identification of Critical Cyber Systems; (3) protecting Critical Cyber Systems; (4) detecting and monitoring Critical Cyber Systems; and (5) and ensuring response and recovery. As discussed above, TSA has added additional requirements emphasized in the CISA CPGs, including cybersecurity training and supply chain risk management requirements, not previously addressed in the SDs.

Consistent with the NIST CSF, the proposed requirements for a COIP represent TSA's target cybersecurity outcomes for the owner/operators that would be subject to the proposed rule. While TSA is committed to providing maximum flexibility for owner/operators to develop CRM programs appropriate for their operations, as provided by the SDs, the proposed rule includes additional requirements that push owner/operators

to the level of cybersecurity maturity that is repeatable. These requirements include more specificity in the type of information to be included in the COIP. Establishing a minimum baseline of information to be included in COIP is necessary to ensure enforceability from the perspective of a regulator, but also enhances communication to employees to ensure they know their responsibilities under the CRM program and that the program and its policies are understood across the organization.

Finally, the proposed requirements for a CRM program include an assessment requirement that aligns with the NIST CSF's taxonomy to achieve maturity by assessing progress toward the target state. The proposed CAP requirements expand upon the requirement for assessments in the SD Pipeline-2021-02 and SD 1580/82-2022-01 series. Under the proposed rule, owner/operators would continue to be required to have a CAP approved by TSA that includes a biennial cybersecurity architecture design review, other assessment capabilities, and annual review of the effectiveness of at least one-third of all required measures in the COIP, so that 100 percent of the policies, procedures, measures, and capabilities and all Critical Cyber Systems would to be assessed at least once over 3 years, with a minimum of 30 percent each year. The rule proposes adding additional requirements to ensure independence of auditors and assessors, reporting results to TSA and corporate leadership, and updates to the COIP based on assessment results.

Subsidiaries. Proposed §§ 1580.303(b), 1582.203(b), and 1586.203(b) specifically address the issue of subsidiaries and allow for business with multiple businesses or business units to submit one CRM program for a single corporate entity. Any documents required by the proposed rule, however, would need to clearly identify and distinguish application of the requirements for each business unit. To meet this requirement, TSA would need to be able to review the plan and readily identify how the requirements are being applied to each business unit. In other words, CRM program documents that require TSA to develop a separate analysis to determine how the

requirements are applied within each business unit would not be acceptable or approved by TSA as meeting the proposed regulatory requirements.

D. Specific CRM program requirements

1. Cybersecurity evaluation (proposed §§ 1580.305, 1582.205, and 1586.205)

The NIST CSF (GV.OC and GV.RM) recognizes the importance of a "current profile" that examines the extent to which the owner/operator is achieving the outcomes in the target profile and identify gaps and potential vulnerabilities. For purposes of the requirements in this proposed rule, TSA would expect owner/operators to use the security outcomes identified in the rule, at a minimum, as a basis for the target profile.

The proposed rule specifically requires this evaluation to include both physical and logical/virtual security controls. If the evaluation is limited to logical/virtual controls, the owner/operator may not fully recognize the strengths and weakness of physical security controls being used instead of, or to augment, cybersecurity measures. For example, if an owner/operator is relying on controls that limit an individual's access to a building or a floor to offset the impracticability of applying MFA to certain systems, it is important to understand how effective those physical security controls are at meeting the intended purpose. Similarly, understanding available physical security controls can help an owner/operator identify mitigation measures pending ability to fully reach the required target state.

As noted above, TSA's SDs for pipeline and rail operators included a requirement to conduct a vulnerability assessment.[148] Under proposed §§ 1580.305(b), 1582.205(b), and 1586.205(b), this vulnerability assessment or other similar assessments may be used to comply with the requirement for the initial cybersecurity evaluation as long as it was

[148] *See* section E. of the SD Pipeline 2021-01 series and section D. of the SD 1580-21-01 and 1582-21-01 series.

completed within no more than one year before submission of the owner/operator's COIP. Under paragraph (c) of these sections, the cybersecurity evaluation must be updated annually. While owner/operators would not be required to submit the evaluation to TSA for approval, they would be required to notify TSA within 7 days of completing the profile and make it available to TSA upon request.

2. Cybersecurity Operational Implementation Plan (proposed §§ 1580.307, 1582.207, and 1586.207)

a. General COIP requirements

The COIP required by §§ 1580.307, 1582.207, and 1586.207 is the center of the comprehensive CRM program. As stated in the proposed rule text, TSA would require the COIP to detail the owner/operator's defense-in-depth plan, including physical and logical/virtual security controls, to comply with the requirements specified in subsequent sections. The results of the cybersecurity evaluation should be used at the beginning of the process to inform the development and revisions to the COIP from a broader enterprise-perspective, while the CAP informs revisions to the COIP based on testing the effectiveness of the measures in the COIP as implemented by the owner/operators. The COIP must include specific detail on exactly how the owner/operators meet the requirements for (a) governance; (b) identification of critical cyber systems, network architecture, and interdependencies; (c) procedures, policies, and capabilities to protect Critical Cyber Systems; (d) procedures, policies, and capabilities to detect cybersecurity incidents; and (e) procedures, policies, and capabilities to respond to, and recovery from, cybersecurity incidents, which would include reporting cybersecurity incidents and the CIRP. Each of these components of the COIP will be discussed below.

As most of the owner/operators that would be subject to this proposed rule's requirements are currently required to comply with TSA's cybersecurity SDs, TSA assumes that the COIP for these owner/operators would include detailed descriptions of

what they are currently doing to meet the required security outcomes. To meet the regulatory requirements, these detailed descriptions would need to be more than a summary or a restatement of the regulatory text. If an owner/operator is relying on specific software, the COIP should provide details on the software (name, version, scope of deployment, etc.). If relying on policies or procedures identified in other corporate documents, the owner/operator would need to specifically identify the sections of those documents, describe how they meet the required security outcomes, and incorporate the specific sections by reference into their COIP.

To the extent the cybersecurity evaluation or CAP identify areas where the owner/operator is not meeting the required security outcomes, the owner/operator would be required by paragraph (d) of §§ 1580.307, 1582.207, and 1586.207 to include a Plan of Action and Milestones (POAM) in their COIP. Incorporating a POAM in the COIP aligns with the identification of remediation measures in section E.1.c. of SD Pipeline-2021-01 series and section D.2. of SD 1580-21-01 and SD 1582-21-01 series. The proposed POAM requirement also aligns with the NIST CSF, which recommends that organizations determine which actions to take to address gaps identified through assessments to achieve the Target Profile.[149] The POAM must include the specific measures to be implemented and a detailed timeframe, not to exceed 3 years, to meet all required outcomes, as well as any mitigating measures that will be implemented pending full compliance with all requirements and security outcomes. As part of the COIP, failure to meet the milestones in the POAM could result in a range of enforcement actions.[150]

The COIP must be made available to TSA for approval. Once approved by TSA,

---

[149] *See supra* note 13 at 7, 11.

[150] *See* TSA's Enforcement Sanction Guidance Policy (last updated Nov. 14, 2022) for more information on TSA's sanction policies, available at https://www.tsa.gov/sites/default/files/enforcement_sanction_guidance_policy.pdf (last accessed June 28, 2023); *see also* TSA Action Plan Program (effective Aug. 26, 2019), available at https://www.tsa.gov/sites/default/files/action_plan_program.pdf (last accessed June 28, 2023).

the COIP is a TSA-approved security program. The proposed rule would require the COIP to be updated to reflect any vulnerabilities or weaknesses identified during the annual cybersecurity evaluation and the CAP, discussed below. In addition, owner/operators would be required to conduct exercises of CIRPs (required by proposed §§ 1580.327, 1582.227, and 1586.227). The results of the exercises must also inform updates to the CIRP as part of the COIP. Whether resulting from these assessments and exercises—or due to other changes in policies, procedures, capabilities, or Critical Cyber Systems—owner/operators would need to comply with the procedural requirements for security programs, discussed below in section III.F. of this NPRM, to revise their COIP.

TSA recognizes that cybersecurity is ever changing in response to new capabilities and emerging threats. In addition, a detailed defense-in-depth plan is likely to include information that is subject to change for a range of reasons. In section 1570.107(c), TSA provides for this possibility by distinguishing between (1) administrative or clerical changes, (2) substantive but temporary changes, and (3) substantive and permanent changes.[151] Within the context of the CRM program, substantive and permanent changes include changes to policies, procedures, or measures contained in a TSA-approved COIP, including documents incorporated by reference into the COIP, that relate to how the owner/operator meets the proposed CRM program requirements and are intended to be in place for 60 or more days. Substantive changes to the COIP must be made following the procedures in proposed § 1570.107(b) for amendments to security programs. For example, a limited-time deployment of new equipment as part of a 30-day pilot may not require amending the CIP, but would require an initial notification to TSA and, within seven calendar days, a description of interim measures that are in place to ensure no diminution of security. A decision to permanently replace equipment would likely require additional measures or revisions to the COIP and

[151] *See* discussion in Section III.F.1. regarding security program amendments in general.

the owner/operator would need to request an amendment.

TSA is not proposing to require owner/operators to follow the amendment process for administrative or clerical changes to COIPs, including administrative or clerical changes to documents incorporated by reference. In other words, administrative or clerical changes do not require a request to TSA, notification to TSA, or TSA approval. Administrative or clerical changes are limited to changes to policies, procedures, or measures contained in a TSA-approved COIP, including documents incorporated by reference, that do not relate to how the owner/operator meets the CRM program requirements. Owner/operators would be required to keep a chronological list of all administrative or clerical changes and when they occurred. This list should be consulted by the owner/operator on a regular basis to determine if any changes may have evolved into permanent changes requiring an amendment.

The following are examples of substantive changes requiring an amendment:

- Changes in policies, procedures, or capabilities made after a determination that a specific policy, procedure, or measure in the COIP is ineffective based on results of the audits and assessments required under the proposed rule;
- New or additional capabilities the owner/operator has identified or obtained for meeting the requirements for a CRM program that have not been previously approved by TSA;
- Additions, modifications, and deletions to lists of Critical Cyber Systems;
- Changes to the method of MFA required to access a Critical Cyber System;
- Updates to the risk methodology for determining criticality of security patches and updates;
- Use of new vendors, companies, or products when they change the process the owner/operator is using to meet a requirement for the CRM program; and
- Strategic network architecture changes, such as moving from segmenting OT

systems with firewalls to using a one-way diode or moving to a zero-trust architecture from a defense-in-depth architecture.

Examples of administrative or clerical changes to COIPs or documents incorporated that do not require the amendment process in § 1570.107(b) could include, but are not limited to the following:

- Changes to names of documents (for example, changing "IT Policy – Monitoring" to "IT Policy – Monitoring, Detection and Auditing");
- When only certain parts of a document are incorporated by reference, changes are made to other parts of a document which are not specifically incorporated by reference; and
- Changes intended to be in effect for less than 60 calendar days (which would be subject to the process for temporary changes under proposed § 1570.107(c)(2)).

TSA would also encourage owner/operators to avoid having to make amendments related to documents incorporated by reference in their COIPs by specifically indicating which sections of the documents are being used to meet the requirements for a CRM program rather than referencing the document in its entirety when only specific portions are relevant.

Under §§ 1580.307(e)(1), 1582.207(e)(1), and 1586.207(e)(1), owner/operators must make their COIP available to TSA in a form and manner prescribed by TSA. TSA decided not to propose a specific method in the NPRM due to the need to remain flexible and adaptive to options for submitting documents. Since first imposition of the SD Pipeline-2021-02 series, TSA has been able to move from only one option (submission through a password protected e-mail or uploading to a secure location using the Homeland Security Information Network (HSIN)) to multiple options, including e-mail/HSIN, a secure portal, and local retention. These options address the concerns of the industry to protect highly sensitive information. While not proposing to codify any of

these options, the following discusses each option as they currently exist.

As noted above, owner/operators were originally required to send their list of Critical Systems, CIP and CAP using email as password-protected attachments or upload to HSIN. TSA subsequently developed other authorized methods for submitting and maintaining CIPs, and documents incorporated by reference into CIPs, CAPs, and CAP reports. Instead of submitting these documents via password-protected email or via HSIN, owner/operators may submit documents to the TSA Secure Regulatory Portal (SRP) or retain them locally for in-person or other review pursuant to TSA-approved methods, which may include virtual review.

Use of the SRP is the preferred method for TSA as it minimizes the time and personnel investment for owner/operators while accelerating TSA's ability to review and approve submitted documents while maintaining information security. Owner/operators would be required to use the same method of submission for all of their required documents and must notify TSA of their chosen option. If documents are maintained locally for on-site or virtual review by TSA, the owner/operator must attest to TSA (subject to potential penalties for providing false or misleading information) that they have completed the required actions within the designated timeline. The documents are considered conditionally approved and the owner/operator must begin implementation. TSA considers "implementation" of the CIP to mean that the regulated entity has fully developed its CIP to meet the performance-based measures and has begun to carry out the policies, procedures, measures, and capabilities in the CIP. Therefore, that attested-to and complete CIP may also include timelines for implementation of specific cybersecurity measures that will achieve the performance-based objectives. A CIP maintained on location is not considered to have final approval until reviewed by TSA, revised as required by TSA, and the owner/operator receives notification from TSA that the CIP has received final approval. Only final approval of the CIP triggers the timelines

associated with requirements to develop the CAP and CAP report. Regardless of the manner of submission of any document, TSA retains its full inspection authority.

TSA has not required any owner/operator to resubmit information previously approved. The required plans and reports submitted to TSA are Federal records and must be retained in accordance with TSA's National Archives and Records Administration (NARA)-approved records schedules. Similarly, documents submitted via the secure portal are also Federal records and must be retained in accordance with same NARA-approved records schedules once TSA reviews them. Finally, documents maintained at an owner/operator's location are not considered Federal records. At this time, TSA intends to continue allowing all of these approved methods for the COIP, CIRP, and CAP.

b. Governance of the CRM program (proposed §§ 1580.309, 1580.311, 1582.209, 1582.211, 1586.209, and 1586.211)

Accountable executive (paragraph (a) of §§ 1580.309, 1582.209, and 1586.209). Both the NIST CSF and the CISA CPGs stress the importance of establishing governance for a CRM program. CPG 1.B. urges identifying a single leader who "is responsible and accountable for cybersecurity within an organization." Specifically, the CISA CPGs recommend that organizations have a named role/position/title identified "as responsible and accountable for planning, resourcing, and execution of cybersecurity activities. This role may undertake activities such as managing cybersecurity operations at the senior level, requesting and securing budget resources, or leading strategy development to inform future positioning." To the extent possible, this individual should not be the Cybersecurity Coordinator or otherwise have responsibility for day-to-day management of the IT or OT system, but should function at a level between the most senior-executive leadership and the implementation/operations level of the organization.[152] CISA has

[152] *See* NIST CSF, *supra* note 13, at 1210-11.

identified this action as one with high impact and low complexity, noting that failure to identify an accountable executive can result in a lack of accountability, investment, or effectiveness of a CRM program.[153]

TSA is adopting this recommendation for purposes of this proposed rule by requiring covered owner/operators to identify an accountable executive for the CRM program. Contact and identifying information for the accountable executive must be provided to TSA and incorporated into the COIP.

Identifying positions with cybersecurity responsibilities (paragraph (b) of §§ 1580.309, 1582.209, and 1586.209). The NIST CSF and the CISA CPGs also emphasize the importance of having a clear understanding of cybersecurity roles and responsibilities within the organization and with stakeholders, and establishing a relationship to ensure effective communication on cybersecurity policies and risks.[154] Consistent with these priorities, TSA is proposing to require the COIP to identify positions designated to manage implementation of policies, procedures, and capabilities described in the COIP and coordinate improvements to the CRM program.

In addition, the proposed rule would require identification of any authorized representatives, as defined in the TSA Cybersecurity Lexicon, responsible for implementation of any part of the owner/operator's CRM program. Authorized representatives are empowered to act on the owner/operator's behalf to coordinate and conduct activities required by this proposed rule, including specific security measures in the owner/operator's TSA-approved COIP. Considering these responsibilities, authorized representatives are liable for non-compliance separate from and in addition to the owner/operator. TSA is proposing to require that the corporate or official business information for all authorized representatives must be incorporated into the COIP and be

---

[153] *See* CISA CPG Checklist, v1.01, available at https://www.cisa.gov/sites/default/files/2023-03/cisa_cpg_checklist_v1.0.1_final.pdf (last accessed Sept. 22, 2023).
[154] *See* NIST CSF GV-RR and CPGs 1.B and 1.C.

supported with written documentation, such as contractual agreements, between the owner/operator and the authorized representative detailing the scope of responsibilities as related to the measures identified in the COIP. As with other documentation requirements, the owner/operators would need to identify specific provisions applicable to the COIP within any provided documentation.

Note that the definition of "authorized representative" in the TSA Cybersecurity Lexicon excludes entities that functions as "Managed Security Service Providers." If an owner/operator, or its authorized representative, has delegated or shared responsibility with a Managed Security Service Provider, wholly or in part, for specific security measures, the owner/operator or authorized representatives retains responsibility for ensuring the application of the cybersecurity performance-based measures.

The distinction in liability between authorized representatives and Managed Security Service Providers is generally consistent with principles of agency. Managed Security Service Providers are not direct employees of the owner/operator but provide one or more services or capabilities that the owner/operator may use to perform required security measures. Managed Security Service Providers generally provide a logical service that is widely available to anyone who purchases the specific capability or service, such as an internet service provider, a program developer, or IT or OT system monitoring and detection capabilities. The authorized representative is an agent empowered to act on behalf of the owner/operator, such as for day-to-day management of a cybersecurity program.

Cybersecurity coordinator (§§ 1580.311, 1582.211, and 1586.211). The proposed rule would codify Section A. of the SD Pipeline-2021-01, SD 1580-21-01 and SD 1582-21-01 series, which requires covered owner/operators to identify a primary and at least one alternate Cybersecurity Coordinator. Security coordinators, in general, are a vital part of transportation security, providing TSA and other government agencies with

an identified point of contact with access to company leadership and knowledge of operations, in the event it is necessary to convey extremely time-sensitive information about threats or security procedures to an owner/operator, particularly in situations requiring frequent information updates. Having a designated Cybersecurity Coordinator and alternate provides TSA with a contact in a position to understand cybersecurity problems; immediately raise issues with, or transmit information to, the designated accountable executive or other appropriate corporate or system leadership; and recognize when emergency response action is appropriate. To meet this purpose, the designated individuals must be accessible to TSA 24 hours per day, seven days per week.

The proposed rule does not change the expectation from the SDs that the Cybersecurity Coordinator (primary and alternate) be appointed at the headquarters level. In addition, TSA would carry over the requirement in the SDs for the primary Cybersecurity Coordinator to be a U.S. citizen who is eligible to receive a security clearance. This requirement is necessary to ensure that TSA can rapidly share sensitive information with the owner/operator that may be critical to ensure appropriate actions are taken to address emerging threats. This requirement is also consistent with the SDs and TSA's experience with Physical Security Coordinators. *See* discussion in Section III.A.2. As with the SDs, the proposed rule would not require the Cybersecurity Coordinator or alternate to be a dedicated position staffed by an individual who has no other primary or additional duties.

The proposed rule would require the following information for the Cybersecurity Coordinator(s): name, title, telephone number(s), and e-mail address. Any change in this information would have to be provided to TSA within seven days of the change taking effect. As previously noted, this is not a new requirement for owner/operators of railroads, including the rail transit operations of PTPR owner/operators, and pipeline facility and systems currently subject to the SDs. If an owner/operator subject to this

proposed rule has provided the required information for primary and alternate Cybersecurity Coordinator(s) to TSA in the past, and that information is still current, no further action would be needed to meet this requirement.

TSA is expanding the requirements for the primary and alternate Cybersecurity Coordinator(s) to ensure they have the knowledge and skills necessary to perform the responsibilities. Cybersecurity is a technical field that requires some degree of knowledge of terms, threats, and the owner/operator's systems in order to be effective.

TSA is specifically requesting comments on existing training and certification programs that could provide low-cost options for meeting these requirements that TSA could review and provide as examples to other owner/operators that would be subject to these requirements.

Updates to governance information. The proposed rule would require owner/operators to notify TSA when information regarding the accountable executive or Cybersecurity Coordinator(s) changes. While the COIP should be current regarding the identification of the accountable executive or Cybersecurity Coordinator(s), TSA would not require the owner/operator to seek an amendment to their COIP to update this information as the updated information would need to be separately provided to TSA.

c. Identification of Critical Cyber Systems, network architecture, and interdependencies

Identifying Critical Cyber Systems (§§ 1580.313, 1582.213, and 1586.213). Both the NIST CSF and the CISA CPGs emphasize the importance of identification of critical assets.[155] As with the applicability determinations for this proposed rule, TSA is proposing an informed, risk-based decision to cybersecurity requirements. A critical first step in this process is risk informed identification of critical IT and OT systems. TSA

[155] *See* NIST ID-AM and CPG 1.A.

included a requirement to identify Critical Cyber Systems in the SD Pipeline-2021-01 and SD 1580/82-2022-01 series.

Identifying Critical Cyber Systems, including both IT and OT systems, enables owner/operators to ensure they have adequately identified risks using multiple sources of information and data to identify the threat (*i.e.*, likelihood of an attack), system vulnerabilities, and consequences should the system be the target of a cybersecurity incident. In general, unless otherwise stated, the cybersecurity measures that would be required for protecting, defending, and responding to cybersecurity incidents are limited to these Critical Cyber Systems.

For purposes of this proposed rule, TSA proposes to incorporate into the TSA Cybersecurity Lexicon a definition of "Critical Cyber System" that includes any IT or OT system used by the owner/operator that, if compromised or exploited, could result in an operational disruption incurred by the owner/operator, including those business support services that, if compromised or exploited, could result in operational disruption. This term includes systems whose ownership, operation, maintenance, or control is delegated wholly or in part to any other party. The definition of an "operational disruption" includes a deviation from or interruption of business critical functions that results in a compromise or loss of data, system availability, system reliability, or control of systems, or indicates unauthorized access to, or malicious software present on, Critical Cyber System.

In addition to IT and OT systems that are obviously critical to operations, owner/operators should also consider programmable electronic devices, computers, or other automated systems which are used in providing transportation; alarms, cameras, and other protection systems; and communication systems, and utilities needed for

security purposes, including dispatching systems.[156] TSA believes the scope of systems to be covered is consistent with the direction in the National Cybersecurity Strategy to ensure cybersecurity regulations "meet the needs of national security and public safety, in addition to the security and safety of individuals, regulated entities, and their employees, customers, operations, and data."[157]

Paragraph (a) of §§ 1580.313, 1582.213, and 1586.213 requires specific identifying information for Critical Cyber Systems. This information, at a minimum, would need to include specific identifying information for the system and manufacturer/designer name for each Critical Cyber System.

TSA recognizes that the owner/operator is in the best position to determine the critical IT and OT systems needed to support its business-critical functions for operations and market (supply chain) expectations. There is, however, also the potential that a cybersecurity incident that may seem minor to a specific owner/operator could have more wide-ranging impacts on the supply chain as well impacts on national and economic security. Paragraph (b) would require the owner/operator to include in its COIP the methodology used for identifying Critical Cyber Systems. Looking at systems and processes based on the business services they support may bring more transparency to, and improve the quality of, decision making, thereby improving overall operational resilience. As part of this methodology, TSA expects owner/operators to use information provided to them on particular risks associated with some systems, including intelligence and other information that identifies the likelihood of a system being the subject of a cybersecurity incident based on known threat information. As noted in the NIST CSF, a mature CRM program is one where the "organization understands its role, dependencies, and dependents in the larger ecosystem," "collaborates and receives information from

---

[156] *See* sections 1531(d)(1)(C) and 1512(d)(1)(C) of the 9/11 Act, codified at 6 U.S.C 1181(d)(1)(C) and 1162(d)(1)(C), respectively.
[157] *See supra* note 12 at 8-9.

other entities," "is aware of the cyber supply chain risks associated with the products and services" it both provides and uses, and "acts formally upon those risks."[158]

While some systems may pose more risk than others, any system that could result in operational disruption should be considered a Critical Cyber System. The methodology would need to describe these considerations and also consider scenarios for how long critical operations and capabilities could be sustained with identified alternatives if a Critical Cyber System is taken offline due to a cybersecurity incident. Finally, once the initial list of Critical Cyber Systems is identified, the methodology would need to include reviewing IT and OT systems not designated as critical to determine the sustainability and operational impacts if one of these systems is unavailable due to a cybersecurity incident. These considerations by the owner/operator may result in needing to update the list of Critical Cyber Systems. Best practices identified by TSA include considering impacts if a system is offline for a short duration (a 4, 8, 12, 24-hour period), or days, a week, several weeks, or months.

It is important to recognize that the availability of backups or "workarounds" should not be considered in determining whether an IT or OT system is a Critical Cyber System. These and other mitigation measures should be considered as part of the COIP as actions that are intended to ensure continuity if a Critical Cyber System is incapacitated. In practice, to the extent an owner/operator has developed backups and other mitigation measures for an IT or OT system, that fact should weigh towards identifying the system as critical, *i.e.,* were it not critical, there would not be a need for robust mitigation measures in the event the system is unavailable.

In §§ 1580.313(e), 1582.213(e), and 1586.213(d), TSA is proposing to incorporate a requirement from the SD for owner/operators to add any IT or OT systems

---

[158] *See* NIST Cybersecurity Framework V1.1. at 10, available at https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (last accessed May 6, 2024); *see also* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1302.ipd.pdf (last accessed May 6, 2024).

identified by TSA as Critical Cyber Systems even if not identified as critical by the owner/operator. While TSA is committed to providing flexibility and allowing owner/operators to self-identify their Critical Cyber Systems, the agency is also committed to ensuring a baseline of cybersecurity across specific modes and similarly situated operations. As a result, if TSA notices that an owner/operator has chosen not to identify a system as critical that was identified by other similarly situated owner/operators, TSA would request additional information and, after consultation with the owner/operator, could require the system to be added. In addition, an owner/operator who does not identify any Critical Cyber Systems is not exempt from the requirements for the CRM program. If TSA agrees that the owner/operator does not have any Critical Cyber Systems, the owner/operator would still need to address other applicable requirements.

Positive Train Control. Consistent with these proposed requirements and standards for identification of Critical Cyber Systems, TSA revised the SD 1580/82-2022-01 series in May 2024 with a new requirement for owner/operators who are either required to install and operate PTC under 49 CFR part 236, subpart I, and/or who voluntarily install and operate PTC under CFR part 236, subpart H or I, to include PTC systems as a Critical Cyber System. TSA is proposing to incorporate this requirement in sections 1580.313 and 1582.213.

PTC helps eliminate the risks of accidents and mishandling of locomotives due to human error by using locomotive-borne devices linked to a central dispatching system, through an integrated network communication channel. PTC systems[159] are designed to

[159] Simply described, PTC systems are comprised of the locomotive onboard computer system, the wayside signals, and the Back Office Server (BOS). Connections are established through cabled cellular communication signals, Wi-Fi, and radio. Some of the data points that are received to control the speed of the locomotive are located through the Global Positioning System (GPS), wayside signal, transponder on or around the track, and monitoring of speed for all locomotives on the same subdivision. Data is compiled from the locomotive into the BOS and is compared to the track image in the PTC system, which can detect violation of movement authority and speed restrictions. The PTC system is an important safety function due to its ability to correct the actions of a train operating outside of the known limits of the system.

prevent train-to-train collisions, over-speed derailments, incursions into established work zones, and movements of trains through switches left in the wrong position.[160]

The imposition of PTC requirements has also resulted in far more interconnected rail systems than previously existed with the potential for a cybersecurity incident to affect multiple operators.[161] The criticality of these systems is reflected in the FRA's regulations that require PTC to be used unless the situation falls within one of the limited exceptions provided in their regulations.[162] TSA is proposing to require rail owner/operators who use PTC to include specific PTC components as Critical Cyber Systems.

As noted above, the FRA's regulations expect PTC to be used unless the situation falls within one of the limited exceptions provided in FRA's regulations. The limited exceptions reflect the criticality of these systems. For example, a train that loses PTC, "[w]here the failure or cut-out is a result of a defective onboard PTC apparatus," while en route may continue "no farther than the next forward designated location for the repair or exchange of onboard PTC apparatuses."[163] The fact that railroads may operate without functioning PTC systems only in limited situations demonstrates the critical need for these systems.[164]

Losing PTC capability is likely to disrupt operations. PTC provides critical safety functions, protecting the public from possible train derailments, misaligned track switches, and head-on collisions. To achieve the intended safety benefits, the PTC

---

[160] *See* FRA, Positive Train Control (PTC), https://railroads.dot.gov/research-development/program-areas/train-control/ptc/positive-train-control-ptc (last accessed Nov. 28, 2023).
[161] In March 2023, a nationwide outage of PTC for Amtrak resulted in cancelled and delayed trains in and out of Chicago for multiple days, affecting Amtrak, commuter railroads, and freight railroads. *See* Bob Johnston, *PTC issues cause Amtrak cancellations and delays*, Trains.com (last updated Feb. 5, 2024), available at https://www.trains.com/trn/news-reviews/news-wire/ptc-issues-cause-amtrak-cancellations-and-delays/ (last accessed Aug. 2, 2024).
[162] *See* 49 CFR 236.1029. Under 49 CFR 236.1029(b)(6), a train that loses PTC en route, "[w]here the failure or cut-out is a result of a defective onboard PTC apparatus," may continue "no farther than the next forward designated location for the repair or exchange of onboard PTC apparatuses."
[163] 49 CFR 236.1029(b)(6).
[164] *See* FRA Information Guide on Positive Train Control, 49 CFR Part 236, Subpart I (dated Dec. 12, 2022).

system must consistently maintain a high level of availability. If the PTC system fails en route, the train must operate at reduced speed and stop at the next forward designated location until the PTC apparatuses are fixed or replaced. Accordingly, loss of the PTC system could interrupt the railroad's operations. Additionally, if a PTC system were to be the target of a cyberattack that resulted in a widespread disruption in system communication where the result was an inability to initialize communications with multiple locomotives, then trains would have to be held until the issue was resolved or FRA otherwise authorized continued operations.[165]

As in the SD, the proposed rule incorporates an alternative in lieu of applying access control measures, as required by proposed §§ 1580.317(b) and 1582.217(b), for the PTC hardware and software components installed on freight and passenger locomotives if the owner/operator is complying with the requirements in 49 CFR 232.105(h)(1-4) (General requirements for locomotives), 49 CFR 236.3 (Locking of signal apparatus housings), or 49 CFR 236.553 (Seal, where required).

Network architecture. Paragraph (c) would require owner/operators to identify system information and network architecture for each identified Critical Cyber System. In general, the requirements in paragraphs (c)(1) through (3) align with those in section III.B.1. of the SD Pipeline-2021-02 and SD 1580/82-2022-01 series. TSA is proposing to add two additional requirements for purposes of ensuring effective asset identification and management as part of a comprehensive CRM program. First, §§ 1580.313(d)(4), 1582.213(d)(4), and 1586.213(c)(4) would require an owner/operator to identify the baseline of acceptable communications between Critical Cyber Systems and external connections, or between IT and OT systems. This requirement is necessary to ensure the owner/operator can comply with requirements in proposed §§ 1580.323, 1582.223, and 1586.223, which require documenting any communications between IT and OT systems

[165] *Id.*

and an external system that deviate from the identified baseline of communications.

Sections 1580.313(d)(5), 1582.213(d)(5), and 1586.213(c)(5) would require the owner/operator to identify any operational needs that prevent implementation or delay implementation of the CRM program requirements for Critical Cyber Systems, such as application of security patches and updates, encryption, or MFA.

Sections 1580.313(f), 1582.213(f), and 1586.213(e) would provide that any substantive changes to Critical Cyber Systems would require an amendment to the COIP. It is critical for both TSA and the owner/operator to know the COIP has the current list of Critical Cyber Systems. TSA prepares for inspections in advance, and it increases the amount of time inspections take for owner/operators and TSA if the list is not current. In addition, having ready access to this information can help TSA notify owner/operators if specific intelligence or other threat information becomes available relevant to that specific system or capability.

Supply chain risk management (§§ 1580.315, 1582.215, and 1586.215). Both the NIST CSF[166] and the CISA CPGs[167] include recommendations related to supply chain risk management. TSA is proposing to incorporate all three recommendations from the CISA CPGs for supply chain risk management into this proposed rule. The requirements would apply to any procurement or contractual documents executed or updated after the effective date of the final rule.

The SolarWinds supply chain compromise is one of the most well-known examples of a cybersecurity risk associated with services and systems provided by external supply chain providers. Using a backdoor implanted in a software update downloaded by customers using the SolarWinds Orion product, malicious actors were able to retrieve and execute commands that included the ability to transfer files, execute

[166] *See* GV.SC. of the NIST CSF.
[167] *See* CPG 1.G, 1.H, and 1.I.

files, profile the system, reboot the machine, and disable system services. The malware masqueraded its network traffic as the Orion Improvement Program-protocol and stored reconnaissance results within legitimate plugin configuration files allowing it to blend in with legitimate SolarWinds activity. The backdoor used multiple obfuscated blocklists to identify forensic and anti-virus tools running as processes, services, and drivers. Victims included government, consulting, technology, telecom and other entities in North America, Europe, Asia and the Middle East.[168]

Proposed §§ 1580.315(a), 1582.215(a), and 1586.215(a) address these supply chain threats by incorporating the recommendations in CPG 1.G, which encourage organizations to incorporate supply chain incident reporting in their procurement documents and contracts to ensure they can more rapidly learn of, and respond to, known cybersecurity incidents across vendors and service providers. Specifically, CPG 1.G recommends that these documents, such as service-level agreements, "stipulate that vendors and/or service providers notify the procuring customer of security incidents within a risk-informed time frame as determined by the organization." A risk-informed timeframe is one that is sufficient for the owner/operator to identify and address any potential risks to their Critical Cyber Systems based on the scope and type of cybersecurity incident.

Paragraph (b) incorporates CPG 1.H, which recommends that organizations require these documents to stipulate that vendors and/or service providers notify the procuring customer of confirmed security vulnerabilities in their assets within a risk-informed time frame. This reporting ensures organizations can more rapidly learn about, and respond to, vulnerabilities in assets provided by vendors and service providers.

---

[168] *See* Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor (Dec. 13, 2020; last updated May 12, 2022) available at https://www.mandiant.com/resources/blog/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-back (last accessed June 12, 2023); *see also* https://www.cisa.gov/news-events/news/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure for more resources regarding the SolarWinds supply chain compromise.

Paragraph (c) incorporates CPG 1.I, which recommends that "procurement documents include cybersecurity requirements and questions, which are evaluated in vendor selection such that, given two offerings of roughly similar cost and function, the more secure offering and/or supplier is preferred." Implementing this recommendation would reduce risk by ensuring that the most secure products and services are purchased and purchasing priority given to more secure suppliers. In its CPG Checklist, CISA has assessed the complexity of these three actions as low, but with high impact at addressing the known threat.

In paragraph (d), TSA is proposing that when a notification of a cybersecurity incident or vulnerability is received, the owner/operator must consider mitigation measures sufficient to address the resulting risk to Critical Cyber Systems. In addition, if any of these measures would result in permanent changes, the owner/operator would need to request to amend its COIP. If the vendor's cybersecurity incident puts the owner/operator's IT or OT systems at more direct and immediate risk, it may also be a reportable cybersecurity incident.

In setting cybersecurity regulations for critical infrastructure, the National Cybersecurity Strategy encourages regulators "to drive the adoption of secure-by-design principles."[169] TSA is requesting specific comments on whether the supply chain requirements in the final rule should also include ensuring that any software purchased for, or installed on, Critical Cyber Systems meets CISA's Secure-by-Design and Secure-by-Default principles.[170]

d. Procedures, policies, and capabilities to protect Critical Cyber Systems

---

[169] *See supra* note 12 at 8-9.

[170] For more information on these principles, *see Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by- Design and -Default* (Apr. 13, 2023), available at https://www.cisa.gov/sites/default/files/2023-06/principles_approaches_for_security-by-design-default_508c.pdf (last accessed Aug. 7, 2023).

Protecting Critical Cyber Systems requires a combination of controls, capabilities, and awareness. Proposed §§ 1580.317, 1582.217, and 1586.217 include the requirements for network segmentation, capabilities to control access to or disruption of OT and IT systems, patch management, and ensuring these capabilities have robust logging and back-up requirements. Proposed §§ 1580.319, 1582.219, and 1586.219 require training to enhance awareness for individuals regarding their role and responsibilities in protecting Critical Cyber Systems.

Network segmentation, controlling communications, zone boundaries, and encryption. Proposed paragraphs (a) through (c) of §§ 1580.317, 1582.217, and 1586.217 would require owner/operators to incorporate into their COIP the network segmentation policies and controls necessary to address cybersecurity threats. To align with the NIST CSF's "Protect" function, this section includes requirements from both section III.B. and section III.C. of the SD Pipeline-2021-02 and 1580/82-2022-01 series.[171] The scope of the requirements in paragraphs (a) through (c) specifically include security outcomes intended to (a) protect against access to, or disruption of, the OT system if the IT system is compromised or vice versa; (b) ensure IT and OT system-services transit the other only when necessary for validated business or operational purposes; (c) secure and defend zone boundaries to defend against unauthorized communications between zones and prohibiting OT services from traversing the IT system, or vice versa, unless encryption or other controls are in place; (d) and control access to Critical Cyber Systems.

Many historical intrusions demonstrate that adversaries generally compromise a single vulnerable system or host and then move laterally across a network until reaching an identified target. Implementing segmentation impedes adversaries who have

---

[171] These requirements generally align with the recommendations in PR-AA of the NIST CSF and CPG 2.C (Unique Credentials), 2.D (Revoking Credentials for Departing Employees), 2.E (Separating User and Privileged accounts), and 2.H (Phishing-Resistant Multifactor Authentication (MFA)), 2.K (Strong and Agile Encryption), 2.0 (Document Device Configurations), 2.P (Document Network Topology), and 2.X (Limit OT Connections to Public Internet).

successfully entered the environment from producing cascading consequences and limits their ability to impact the entire process simultaneously, reducing both physical and cyber consequences. Network segmentation is necessary to reasonably ensure that an intrusion is limited to the initially compromised host and does not spread to affect Critical Cyber Systems. Flat or unsegmented networks pose an exigent risk to cybersecurity, as any intrusion-spread can result in a significant impact to systems that support public health and safety. Preventing or controlling such spread mitigates the costs of a successful cybersecurity incident, especially if segmentation averts intruder exposure to critical systems, which could potentially cost billions of dollars in damage. Reducing the costly impacts of ransomware attacks over time may change the economic incentive of the attackers and reduce their frequency in the long-term.

Access control. Proposed paragraph (b) of §§ 1580.317, 1582.217, and 1586.217 includes requirements for controlling access to Critical Cyber Systems. These requirements generally align with the recommendations in PR-AA of the NIST CSF and CPG 2.C (Unique Credentials), 2.D (Revoking Credentials for Departing Employees), 2.E (Separating User and Privileged accounts).

As noted above (*see* section III.D.2.c.), TSA is proposing a limited exception for application of access control measures required by proposed paragraph (b). In lieu of these requirements, §§ 1580.317(f) and 1582.217(f) would allow owner/operators to rely on the physical security controls used to comply with the FRA's regulations under 49 CFR 232.105(h)(1-4) (General requirements for locomotives), 49 CFR 236.3 (Locking of signal apparatus housings), *or* 49 CFR 236.553 (Seal, where required), as applicable. This exception is limited to PTC hardware and software components installed on freight and passenger locomotives. TSA previously provided this exception in revisions to the SD 1580/82-2022-01 series issued in June 2024. To rely on this exception, owner/operators would need to be in full compliance with the FRA regulations noted in

the exception and specify in their COIP what physical security measures are being used to prevent unauthorized access to the specific PTC components installed on the locomotive.

Identification and authentication policies. Managing identification and authentication policies are fundamental controls that should be part of a basic cybersecurity program and should already be in place for organizations covered by applicability of the SDs. To the extent that these controls are not in place, this is a vulnerability that could be imminently exploited.

Regularly changing passwords is a fundamental cybersecurity practice. Minimizing this known threat vector requires immediate action to mitigate the threat. VADRs conducted by CISA, and other assessments and interviews with asset owners, have identified cases where passwords used in ICS were stolen, the organization was aware they had been compromised, yet the passwords were subsequently left unchanged for multiple years. In the absence of effective controls, adversaries in possession of these passwords could use them at any time to access the ICS. If at any time passwords were previously compromised and are still valid and have not been disabled or other compensating controls provided to prevent adversarial access to the system, those passwords could be used by an adversary to access the system.

Multi-factor authentication. Multi-factor authentication (MFA) requirements, or compensating controls that meet the same security outcomes, are also critical to provide a critical, additional layer of security to protect asset accounts whose credentials have been compromised. Aggressive activity being demonstrated by threat actors against both IT and OT systems stems from identity management abuse, which can be significantly mitigated by using strong access control measures, such as MFA. Accounts using only a username and password are vulnerable to multiple modes of compromise, including password spraying and credential stuffing. Multi-factor authentication effectively

protects against these tactics and associated unauthorized access. Implementing this requirement reduces the risk of unauthorized access to Critical Cyber Systems by employing security access controls that are equal to or greater than the protection offered by the use of MFA. The intent is to employ MFA where appropriate and, where it is not, to ensure strong physical and logical security controls are in place that meet or exceed the protection that MFA affords.

Similar to the PTC exception for rail operations, TSA is proposing to incorporate from the SD Pipeline-2021-02 series a limited exception for MFA that addresses pipeline-specific operational considerations. In its regulations applicable to the safety of pipeline operations, PHMSA imposes requirements specifically applicable to control rooms used to monitor and control all or part of a pipeline facility through a SCADA system.[172] Under PHMSA's regulations, controllers in the control room are responsible for monitoring day-to-day operations of the SCADA system and managing abnormal and emergency situations. In the midst of an emergency or alarm resolution, requiring MFA to access a workstation could have significant ramifications for pipeline safety and security. Based on these considerations, TSA is proposing to carry forward the limited exception from the SD to proposed § 1586.217(b)(2). Under this exception, if an owner/operator is in compliance with PHMSA's requirements, and includes in its COIP details of the adequate, compensating controls it uses to prevent unauthorized physical and logical access to control room industrial control systems within the scope of the owner/operator's Critical Cyber Systems, it can rely on those measures in lieu of MFA. At a minimum, TSA would expect the COIP to detail physical security controls including segmentation of the workstation from enterprise IT systems and additional compensating

[172] *See, e.g.,* 49 CFR 192.631 (applicable to transportation of gas) and 49 CFR 195.446 (applicable to hazardous liquids). For purposes of these regulations, a control room is defined as "an operations center staffed by personnel charged with the responsibility for remotely monitoring and controlling a pipeline facility." *See* 49 CFR 192.2 and 195.2.

controls applied to prevent unauthorized physical and logical access to the workstation(s).

Privileged accounts. Most intrusions that occur are identity compromises, and implementing these controls greatly reduces the impact from successful compromises by limiting what can be done with any credentials and making intrusions more visible in the use of these credentials. Controlling access to and closely monitoring user accounts is a foundational control necessary to limit the extent of disruption and damage caused by potential intrusions.

Establishing governance over privileged accounts addresses the urgent risk of unauthorized administrative access to life safety systems. Establishing governance over such accounts is a foundational step that should be undertaken to increase the industry baseline for control access. Establishing this baseline of security would significantly reduce the vulnerability of the Critical Cyber Systems because adversaries are currently seeking to exploit entities with weaker access control compared to competitors or the industry standard. Policies such as Just-In-Time Privileged Account Management can mitigate the risk of privileged-account abuse by reducing the amount of time a threat actor has to gain access to privileged accounts before moving laterally through a system and gaining access to sensitive data.

Controlling privileged accounts is an important initial step toward implementing "zero trust" policies. Zero trust is a cybersecurity paradigm focused on resource protection and the premise that trust is never granted implicitly but must be continually evaluated.[173] The purpose of zero trust is to minimize uncertainty in enforcing accurate, least privilege, per-request access decisions for IT and OT systems in the context of assuming that a

[173] *See* NIST SP 800-207, Zero Trust Architecture, at 4 (Aug. 2020). Zero trust architecture is an end-to-end approach to enterprise resource and data security that encompasses identity (person and nonperson entities), credentials, access management, operations, endpoints, hosting environments, and the interconnecting infrastructure. The initial focus should be on restricting resources to those with a need to access and grant only the minimum privileges (*e.g.*, read, write, delete) needed to perform the mission. Document available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf (last accessed Oct. 16, 2023).

breach is inevitable or has already likely occurred.[174] Unauthorized access to privileged accounts can be used to exercise administrative control of highly critical systems, including those that manage life safety functions. Privileged accounts must be well-governed, including by controlling and closely monitoring their use. *Managing shared accounts.* In general, shared accounts are inherently vulnerable to a cybersecurity incident and should never be used. As a result, it is best to require individual user and administrator accounts where technically feasible, with security controls appropriate for the different privilege levels and policies that prohibit sharing accounts. Shared accounts open a security vulnerability and complicate post-incident review of cybersecurity incidents. The vulnerability exists as long as an active password is known by individuals who no longer need access. It is not sufficient to rely on revoked credentials to mitigate the risk when an employee who knows the password no longer needs access to the system. The lack of unique passwords can also be a critical factor in incident response. For example, when accounts are shared among multiple individuals, it may not be feasible to determine which user is responsible for a given action. If a security incident occurs, it can be difficult to identify the source of that incident if it comes from a shared account.

While an ideal CRM program would not permit shared accounts, TSA recognizes that, in some control system environments, management may make a risk-based decision to allow shared accounts. If the owner/operator permits shared accounts in limited situations as determined necessary for operations, that decision needs to be managed with appropriate compensating controls, including capabilities such as enterprise password vaults and/or a logging system that allows the owner/operator to determine who has had access to the account and when. This data is critical for a forensic investigation following a cybersecurity incident. The proposed rule would require the owner/operator

---

[174] *Id.*

to include actions to manage the risks of shared accounts in their COIP.

Trust relationships, especially identity trust relationships between systems, are exploited by adversaries to compromise systems. In environments with shared trust between the OT and IT environments, a compromise to an IT system can immediately and directly place the OT system at risk. Severing these identity trusts is a critical safeguard in light of the current threat. If credentials from a shared or trusted store have been previously comprised, any system that trusts those credentials is put in immediate risk.

Patch management. Proposed paragraphs (e) of §§ 1580.317, 1582.217, and 1586.217 would require owner/operators to have a patch management strategy that ensures all critical security patches and updates are made consistent with the owner/operator's risk-based methodology for prioritizing patches. These requirements align with section III.E. of the SD Pipeline-2021-02 and 1580/82-2022-01 series and CPG 1.E (Mitigating Known Vulnerabilities). Unmanaged software can introduce vulnerabilities into a system and, if left unpatched, could lead to a system compromise. Historical intrusions, including those affecting critical infrastructure, demonstrate that adversaries commonly exploit unpatched or legacy assets. A robust patching program ensures that known vulnerabilities are quickly addressed based upon criticality of the underlying asset. A timely patching program is a fundamental attribute of a mature cybersecurity program and is likely already in place for organizations within the applicability of this proposed rule. Proof of concept exploit codes for critical Windows vulnerabilities are often publicly available and seen "in the wild" within hours/days.

Logging. Proposed paragraph(d) of §§ 1580.317, 1582.217, and 1586.217 would require owner/operators to ensure logging data is stored in a secured and centralized system and maintained for a duration sufficient to support risk analysis. When a cybersecurity incident occurs, the focus is often on recovery to normal operations, but it

is also critical to have strong procedures in place to ensure that critical data is not destroyed that could identify perpetrators and vulnerabilities. Log retention policies enable an organization to determine the scope of an intrusion, protecting the integrity of critical systems and life safety controls.

Numerous recent cybersecurity incidents have indicated that organizations with insufficient logs are unable to effectively identify or assess the extent of a cybersecurity incident. In VADRs conducted by CISA, nearly half of all assessments identified issues related to how logs are kept and maintained, including failures to centrally collect logs and failure to have resources and policies necessary to properly analyze and audit logs. Considering the current capabilities of adversaries as identified in the classified intelligence, owner/operators need to be prepared to determine the scope of an incident to ensure the safety and resiliency of their operations in support of national and economic security. Without this information, organizations often cannot determine whether an actor has penetrated control or digital safety systems.

These requirements would generally align with the requirements in section III.E. of the SD Pipeline-2021-02 and 1580/82-2022-01 series. Both the NIST CSF (PR.PS Function) and the CISA CPGs recognize the importance of logging policies.[175] While CISA recognizes that log collection can be more complex than some of the other requirements, they also note that effectively implementing this control reduces the risk of delayed, insufficient, or incomplete ability to detect and respond to potential cybersecurity incidents.[176]

Back-ups. Proposed paragraph (e) of §§ 1580.317, 1582.217, and 1586.217 would require owner/operators to ensure critical systems are backed up. TSA's SDs required owner/operators to have a CIRP that included security and integrity of backed-

[175] *See* NIST PR.PS Function and CPG 2.T (Log Collection) and 2.U (Secure Log Storage).
[176] *See* CPG Checklist, *supra* note 153.

up data and ensuring that the backed-up data is free from malicious code before it is used to restore a system. For purposes of this rulemaking, TSA is separating this requirement into two sections. The requirement to secure backups would be under the protection portion of the CRM program, while requirements related to using the backups to restore systems would be under measures addressing response and recovery. *See* proposed §§ 1580.327(b)(2), 1582.227(b)(2), and 1586.227(b)(2).

These proposed requirements are consistent with CPG 2.R (System Backups) and the NIST CSF (PR.DS Function). The CISA CPGs recognize the importance of having systems that are necessary for operation backed-up on a regular cadence and ensuring they are stored separately from the source system and tested on a recurring basis.

Cybersecurity Training. Proposed §§ 1580.319, 1582.219, and 1586.219 would require owner/operators to provide two levels of initial and recurrent cybersecurity training. First, basic cybersecurity training must be provided to all employees, including contractors, with access to the owner/operator's IT or OT system and additional training to cybersecurity-sensitive employees. Second, employees who meet the definition of a "cybersecurity-sensitive employee" must receive both basic and role-based cybersecurity training. Consistent with requirements for physical security training, TSA is proposing that individuals who do not receive the required training within the required timeframe must not be allowed access to Critical Cyber Systems or an IT or OT system that is interdependent with a Critical Cyber System. In § 1570.3, TSA is proposing to define "cybersecurity-sensitive employees" as "any employee who is a privileged user with access to, or privileges to access, a Critical Cyber System or any Information or Operational Technology system that is interdependent with a Critical Cyber System as defined in the TSA Cybersecurity Lexicon." Under proposed paragraph (b), owner/operators would be required to include in their COIP a curriculum or lesson plan for each course needed to meet the specific curriculum requirements.

Proposed paragraph (c) of proposed §§ 1580.319, 1582.219, and 1586.219 includes the curriculum requirements for basic cybersecurity training to provide cybersecurity awareness to address best practices, acceptable use, risks associated with their level of privileged access, and awareness of security risks associated with their actions. The requirements in the proposed rule are consistent with CPG 2.I (Basic Cybersecurity Training) and 2.J (OT Cybersecurity Training). All employees should have a basic understanding of the online threat environment. Basic cybersecurity awareness training helps employees understand proper cyber safety, and the security risks associated with their actions. Regular training helps employees recognize their role in cybersecurity and how they serve as an additional "sensor" to detect an incident, regardless of their technical expertise.

Proposed paragraph (c) requires the owner/operator to provide cybersecurity-sensitive employees training that specifically addresses their role as a privileged user to prevent and respond to a cybersecurity incident, acceptable uses, and the risks associated with their level of access and use as approved by the owner/operator. This training recognizes that the level of cybersecurity training for someone with access to critical IT systems may be different than the training needed for someone who primarily accesses critical OT systems. In addition, this training must ensure these employees understand and are prepared to execute any actions associated with their positions under the owner/operator's TSA-approved CIRP.

The proposed schedule for cybersecurity training is consistent with the CISA CPGs. Under paragraph (d) of proposed §§ 1580.319, 1582.219, and 1586.219, owner/operators would be required to provide initial cybersecurity training (based and role-based, as applicable) within 60 days after the effective date of TSA's approval of the COIP. For individuals who onboard or become cybersecurity-sensitive employees after the effective date of the COIP, TSA would require training within 10-days of onboarding.

Paragraph (e) of these sections would require annual recurrent training.

In the CPGs, CISA noted that basic cybersecurity training should be required annually "for all organizational employees and contractors that cover basic security concepts, such as phishing, business email compromise, basic operational security, password security, etc.," and organizations should "foster an internal culture of security and cyber awareness."[177] The CISA CPGs also recommend that all new employees receive this basic initial cybersecurity training within 10 days of onboarding and recurring training on at least an annual basis.[178] For individuals with responsibilities for protecting critical systems, such as maintaining or securing OT system, as part of their regular duties, the CISA CPGs recommend additional cybersecurity training on an annual basis.[179] In the CPG Checklist, CISA identifies these actions as having low complexity and high impact. The CPG Checklist also identifies free services and references that can be used for cybersecurity training.[180] TSA's proposed requirements for cybersecurity training align with the CPG recommendations.

Paragraphs (f), (g) and (h) of proposed §§ 1580.319, 1582.219, and 1586.219 address recognition of prior training and retention of training records. Paragraph (f) specifically allows owner/operators to rely on previously provided cybersecurity training to meet the requirements in the proposed role to the extent they can validate it meets curriculum and schedule requirements in the proposed rule. Paragraphs (g) and (h) include proposed requirements for retention of records and making the record available to employees that are consistent with TSA's current requirements for physical security training of security-sensitive employees (in current 49 CFR 1570.121).

e. Procedures, policies, and capabilities to detect cybersecurity

---

[177] *See* CPG 2.I (Basic Cybersecurity Training).
[178] *Id.*
[179] *See* CPG 2.J (OT Cybersecurity Training)
[180] *See supra* note 153.

incidents (proposed §§ 1580.321, 1582.221, and 1586.221)

As it is not possible to stop all cybersecurity incidents or attempted incidents, it is critical to have strong capabilities to detect cybersecurity incidents when they occur and have automatic measures in place to mitigate the impact. TSA's cybersecurity SDs included specific requirements to ensure continuous monitoring and detection policies.[181] The proposed requirements in §§ 1580.321, 1582.221, and 1586.221 align with the SDs.

A key element of initial access for a cyber-intrusion is the execution of malicious software and communications with malicious command-and-control servers. Implementing filters to ensure "allow-listing" of known, good software and blocking malicious domains are essential controls to prevent damaging intrusions from occurring. In the latter case, best practices, such as protective Domain Name System (DNS) resolution, are necessary to proactively block communications with unknown or potentially malicious web domains.[182] Detection should not be limited to a single security control but should include continuous monitoring and detection policies that follow the zero trust principle of assumed breach and a defense-in-depth approach to maximize a defender's chance of detecting an attack before it reaches the operational environment. Starting with basic controls, such as allow-list filters, email sandboxing, threat-based detection, and protecting DNS, provides a strong foundation for detection of threat activity from advanced adversaries. The costs of implementing these controls would be offset by the benefits of avoiding even a single successful cybersecurity incident that could result in catastrophic costs. The demands of the ransomware threat actors have also increased, and intelligence information indicates the capabilities of adversaries are becoming more sophisticated. The CISA CPGs note that "[w]ithout the knowledge of relevant threats and ability to detect them, organizations risk that threat

[181] *See* section III.D. of the SD Pipeline-2021-02 and 1580/82-2022-01 series.
[182] *See* NIST SP 800-81-2, Secure Domain Name System (DNS) Deployment Guide (Sept. 2013).

actors may exist undetected in their networks for long periods."[183]

f. Procedures, policies, and capabilities to respond to, and recover from, cybersecurity incidents

In setting cybersecurity regulations for critical infrastructure, the National Cybersecurity Strategy encourages regulators to ensure that systems are designed to fail safely and recover quickly.[184] Having strong procedures, policies, and capabilities to respond to, and recover from, cybersecurity incidents are among the most critical steps owner/operators can take. If a company is the target of one of the most sophisticated adversaries, such as nation-state actors, the issue is when the company will be the target of a cybersecurity incident, not whether they will be targeted. These requirements are related to protection and detection capabilities.

Capabilities to respond to a cybersecurity incident (§§ 1580.323, 1582.223, and 1586.223). The detection capabilities discussed above primarily rely on automated systems that flag or block incidents as they occur. CRM programs also need the capability to analyze traffic and trigger responses if certain thresholds are crossed. For this rulemaking, TSA is proposing to consolidate requirements from section D.2 of the SD Pipeline-2021-02 and SD 1580/82-2022-01 series that address auditing unauthorized access, documenting communications between systems that deviate from the approved baseline of communications, identifying and responding to execution of unauthorized code, and ensuring standardized incident response activities based on this information.

Reporting cybersecurity incidents (§§ 1580.325, 1582.225, 1584.107, and 1586.225). TSA's first SD requirements for cybersecurity focused on the need to report cybersecurity incidents to the U.S. government promptly to ensure the government can adequately respond to threats to national security, including economic security.[185] Both

---

[183] *See* CPG 3.A (Detecting Relevant Threats and Tips).
[184] *See supra* note 12 at 8-9.
[185] *See* Sections B-D of the SD Pipeline-2021-01, 1580-21-01, and 1582-21-01 series.

the NIST CSF (Function RS.CO) and CPG 4.A (Incident Reporting) recognize the importance of reporting cybersecurity incidents. In the CPGs, CISA notes that a failure to provide timely incident reporting affects the ability of CISA and other groups to assist the organization and also gain "critical insight into the broader threat landscape, (such as whether a broader attack is occurring against a specific sector)."

TSA is proposing that the requirement to report cybersecurity incidents apply to all owner/operators required to report significant security concerns under current § 1570.203. This applicability would generally include all owner/operators identified in § 1580.1(a)(1), (a)(4), and (a)(5), rail transit and passenger railroads identified in § 1582.1, higher-risk bus-only transit systems identified in § 1582.101, higher-risk OTRB owner/operators identified in § 1584.101, and the pipeline facilities and systems identified in new § 1586.101(b).

The proposed requirements for cybersecurity incident reporting mirror those in the current SDs. As under the SDs, TSA would require owner/operators to report cybersecurity incidents to CISA within 24 hours of identification of a cybersecurity incident.[186] For purposes of the proposed rule, a "cybersecurity incident" is defined as "an event that, without lawful authority, jeopardizes, disrupts or otherwise impacts, or is reasonably likely to jeopardize, disrupt or otherwise impact, the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident on the system." The reports must, among other things, (1) identify the affected systems or facilities; and (2) describe the threat, incident, and impact or potential impact on IT and OT systems and operations. All information reported under this requirement is SSI protected under 49 CFR part 1520 and would be appropriately

[186] As originally issued, the directive required notification within 12 hours of identification. In May 2022, TSA revised this requirement to require notifications within 24 hours of identification.

protected by CISA and TSA.

At the time TSA issued specific requirements for reporting of cybersecurity incidents in 2021, it determined that CISA should receive all cybersecurity incident reporting in order to obtain the security and analytical benefits of consolidating this information in one system to enhance threat identification and trend analysis. This action is consistent with 49 U.S.C. 114(m), which permits TSA to use the services and capabilities of other agencies and to support them through use of the agency's authorities, as appropriate.

TSA is aware that CISA is also required to issue a regulation to require reporting of cyber incidents under the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).[187] Although CIRCIA requires CISA to implement new reporting requirements through regulation, CIRCIA's rulemaking requirement does not supersede, abrogate, modify, or otherwise limit any authority to regulate or act with respect to the cybersecurity of an entity vested in any U.S. Government officer or agency.[188] "Covered Entities," as defined by CISA, that are obligated to report "Covered Cyber Incidents" or "Ransom Payments" pursuant to another federal regulatory requirement, directive, or similar mandate could remain obligated to do so. TSA is, however, committed to avoiding redundancy and harmonizing with our government partners on cybersecurity requirements.

Under the structure proposed by CISA in its NPRM,[189] TSA does not anticipate the need to make any significant modifications to its reporting requirements. TSA will continue to require reporting to CISA to avoid duplicate reporting. If CISA's final rule includes the proposed requirement for agencies to enter into an agreement with CISA to

---

[187] *See* Division Y of Public Law 117-103, 136 Stat. 1039 (Mar. 15, 2022), as amended by Public Law 117-263, 136 Stat. 3661 (Dec. 23, 2022), as codified at 6 U.S.C. 681 – 681g.
[188] 6 U.S.C. 681b(h).
[189] *See* 89 FR 23644 (Apr. 4, 2024) (proposed rule); 89 FR 37141 (May 6, 2024) (comment period extension); 89 FR 47471 (June 3, 2024) (correction).

specifically address duplicative information reporting, TSA believes it is well-positioned for this step based on its current reporting requirements. As CISA is likely to finalize the CIRCIA rule before this rulemaking is finalized, TSA will review the final CIRCIA requirements for reporting cybersecurity incidents and consider changes as necessary and/or appropriate in the final rule.

Cybersecurity Incident Response Plan (§§ 1580.327, 1582.227, and 1586.227). Incident planning and preparedness is critical to mitigating the impacts of a cybersecurity incident on national security, including economic security. The NIST CSF (PR and RC Functions) and CPG 2.S (Incident Response (IR) Plans) and 5.A (Incident Planning and Preparedness) both recognize the importance of having a plan that is tested, validated, and maintained to ensure timely response to, and recovery from, detected cybersecurity events that cause, or could cause, operational disruption. This proposed rule would incorporate the CIRP requirements from section III.F. of the SD Pipeline-2021-02 series and section C.1. of the SD 1580-21-01 and 1582-21-01 series. These requirements include having a plan to ensure that each of the following objectives are met: (1) the impacts of a cybersecurity incident that causes, or could cause, operational disruption or significant impacts on business-critical functions are limited and do not spread throughout the system; (2) back-up data is tested before it is used for recovery; (3) measures are in place to ensure isolation of technology to reduce risks; and (4) identification of who, by position, is responsible for implementing measures in the plan. The SDs also require owner/operators to conduct annual exercises of their plans that, at a minimum, test at least two of these objectives each year. The overall objective of the exercise requirement is to ensure that elements of the incident response plan are tested to ensure that they will work and can be properly executed by the responsible person(s).

As recommended by CPG 2.S (Incident Response Plans), which aligns with the NIST CSF (Function RS.MA), TSA would continue to require owner/operators to test

their plans through exercises and modify the CIRP within 90 days based on the results of the exercises. While the CIRP required by this proposed rule would be incorporated into the COIP made available to TSA for approval, TSA would require that any changes to the CIRP be reported to TSA within 15 days. As these changes are separately reported to TSA, revisions to the CIRP do not require an amendment to the COIP under § 1570.107 of the proposed rule.

3. Cybersecurity Assessment Plan (proposed §§ 1580.329, 1582.229, and 1586.229)

As discussed above, the NIST CSF, the CISA CPGs, and TSA's SDs, taken in their totality, recognize the importance of having cybersecurity measures informed both by an initial cybersecurity evaluation that looks at the current profile of the owner/operator's cybersecurity measures against the target profile, and an assessment program that actually tests the effectiveness of cybersecurity measures in the COIP as related to Critical Cyber Systems. In the initial SD issued to pipeline owner/operators, SD Pipeline-2021-01, TSA required owner/operators to have a third-party conduct a cybersecurity architecture design review.

In SD Pipeline-2021-02C, issued in July 2022, TSA modified the SD to require owner/operators to have a Cybersecurity Assessment Program that allowed owner/operators to conduct their own biennial cybersecurity architecture design review and also required them to use other assessment capabilities intended to test the effectiveness of their cybersecurity measures. Owner/operators were required to have an annual plan for these assessments and to submit the plan to TSA for review, but not for approval.[190]

In July and October 2023, TSA modified the pipeline and rail SD series, respectively, to change the name from a Cybersecurity Assessment Program to a

[190] *See* Section III.G. of the SD Pipeline-2021-02 series and Section III.F. of SD 1580/82-2022-01 series.

Cybersecurity Assessment Plan, which more accurately reflects additional changes made to the requirements. Under the current SD series, owner/operators must submit the CAP to TSA for approval. The CAP must include a specific schedule for the assessments to ensure that at least one-third of the COIP is tested each year at a pace to ensure 100 percent of the policies, procedures, measures, and capabilities in the COIP are assessed over any 3-year period as applied to all Critical Cyber Systems. The intent of this requirement is to ensure a continuous process of assessment, avoiding the potential vulnerabilities that could result from failing to only conducting assessments every few years, potentially leaving vulnerabilities undetected for years.

This proposed requirement gives owner/operators flexibility in developing their CAP schedule. One approach would be to assess/audit one-third of the policies, procedures, measures and capabilities in the CIP each year for all Critical Cyber Systems. Another acceptable option, however, would be to assess/audit one-third of Critical Cyber Systems each year for all applicable policies, procedures, measures and capabilities in the COIP.

Either of these options ensures a schedule where one-third of policies, procedures, measures, and capabilities in the COIP are assessed each year with 100 percent of the policies, procedures, measures, and capabilities in the COIP being assessed/audited every 3 years on 100 percent of the Critical Cyber Systems. Under this requirement, an owner/operator who chooses to assess more than one-third in one year, is still required to assess at least one-third the next year. For example, if the owner/operator assesses 100 percent of their measures in Year 1, at least one-third would need to be assessed again in Year 2 and Year 3 of the cycle.

TSA is specifically requesting comment on methods owner/operators would use to ensure this schedule is met. Smaller companies with fewer Critical Cyber Systems that find it easier to assess 100 percent each year could submit a CAP that includes different

types of assessments each year, *i.e.,* assessing 100 percent each year using different methodologies.

To ensure both the owner/operator and TSA have a clear agreement on the planned assessment program and that it will meet the requirements by the end of the three-year period, TSA is proposing to require the CAP to include a mapping sufficient to validate that the required scope of the assessment will be met within the required period. This step is necessary as TSA recognizes that neither all parts of the COIP nor all Critical Cyber Systems are equal, and it may not be possible to identify a bright line of one-third of the COIP being assessed each year. Mapping the scheduled assessments to the COIP and Critical Cyber Systems will enable TSA and the owner/operator to engage in a discussion to ensure the proposed rule's intent, a steady state of meaningful assessments, is built into the owner/operators CRM program and informing future modifications to improve cybersecurity. TSA assumes that the first mapping will be the most burdensome, requiring minor updates in future years to address any changes in the COIP or Critical Cyber Systems.

TSA also agrees with the CISA CPGs' recommendation that, whenever possible, auditors and assessors should be from outside the owner/operator's organization.[191] At the same time, TSA recognizes that some companies may have in-house capabilities to conduct audits and assessments. Rather than requiring a third-party validator, TSA is requiring that any individual who conducts an audit or assessment must be independent, *i.e*., they must not have a vested or other financial interest in the results, in order to ensure the integrity and reliability of results. For example, if an individual conducting an audit is part of a team or group that would receive a bonus if the audit results met a certain threshold, they are not sufficiently independent to be eligible to conduct the audit.

To support overall governance of the CRM program, the proposed rule would

---

[191] *See* CPG 1.F (Third-Party Validation of Cybersecurity Control Effectiveness).

require an annual report of the CAP results. This report must also include the methodologies used. A copy of the report must be provided to corporate leadership and TSA. Under paragraph (f) of §§ 1580.307, 1582.207, and 1586.207, the results of this assessments are to be used for updating the CRM program, as appropriate. TSA is proposing that the report be provided 15 months from the date of TSA's approval of the first CAP and annually thereafter. This timeline allows for full implementation of the CAP (an annual or 12-month plan), and three additional months to develop a report based on the results. The proposed rule text specifically notes that the audits and assessments conducted under this section are vulnerability assessments subject to the SSI protections in 49 CFR part 1520.

The procedures discussed for submission of CIPs in section III.D.2.a. also apply to submission of CAPs. As with CIPs, a CAP maintained at the owner/operator's location is not considered to have received final approval until reviewed by TSA, revised as required by TSA and the owner/operator receives notification from TSA that the CAP has received final approval. Only final approval of the CAP triggers the timelines associated with subsequent annual requirements to develop the CAP and CAP report.

4. Documentation to establish compliance (proposed §§ 1580.331, 1582.231, and 1586.231)

In accordance with 49 U.S.C. 114(f) and 49 CFR part 1503, TSA may view, inspect, and copy records, in carrying out TSA's security-related statutory or regulatory authorities, including its authority to enforce security-related laws, regulations, directives, and requirements. At the request of TSA, each owner/operator subject to the requirements of the proposed rule must provide evidence of compliance, including copies of records if requested, sufficient to demonstrate compliance. TSA must be able to build and preserve a sufficient administrative record for each case.

For the specific purposes of the CRM program requirements, the proposed rule

includes a section on documentation that TSA may ask to review to establish compliance. The list of documentation provided aligns with the lists in section IV.C of the SD Pipeline-2021-02 and 1580/82-2022-01 series. While TSA has the authority under 49 U.S.C. 114(f)(7) to review any documents necessary to enforce security-related regulations and requirements (among other purposes), TSA provided this non-exclusive list to provide owner/operators with examples of the types of documents TSA may ask to review in order to support the owner/operator's efforts to establish compliance.

E. Physical security

As noted above, TSA is reorganizing 49 CFR parts 1570, 1580, 1582, and 1584 through this rulemaking, to distinguish between physical security requirements and cybersecurity requirements. The security measures previously imposed for rail, PTPR, and OTRB—security coordinators, reporting significant security concerns, security training, and chain of custody (for freight railroads)—are primarily intended to address physical security concerns, *i.e.,* threats to physical infrastructure from improvised explosive devices or physically tampering with equipment. With this rulemaking, cybersecurity requirements would receive dedicated treatment.

To help distinguish between physical and cybersecurity, the rule proposes to generally include the physical and cybersecurity requirements in separate subparts applicable to each mode. The requirements for OTRB would continue to be in subpart B of part 1584. TSA would also distinguish between (1) requirements for Physical Security Coordinator(s) and reporting physical security concerns and (2) requirements for Cybersecurity Coordinator(s) and reporting cybersecurity incidents.

To clearly establish the distinction between physical security and cybersecurity, TSA is proposing to move the security coordinator requirements in current § 1570.201 and reporting requirements in current § 1570.203 to the modal-specific parts with only one change to the current requirements. As with the Cybersecurity Coordinators required

under the CRM program, TSA is specifying that the Physical Security Coordinator(s) be a U.S. citizen unless this requirement is waived by TSA.[192] TSA would consider several factors before waiving this requirement. Most importantly, the individual would need to successfully complete an STA. In addition, TSA would need to ensure that at least one of the owner/operator's Physical Security Coordinator(s) (primary or alternate) is a U.S. Citizen who is eligible for a security clearance. This requirement is consistent with current practice and, as previously discussed, necessary to ensure that there is at least one point of contact within every covered entity that TSA can share sensitive information with on a rapid basis. This information could not be shared with non-citizens absent significant coordination at a government-to-government level. The delay caused by this coordination could prevent an owner/operator from receiving critical information on a timely basis needed to protect against actionable intelligence at a classified level.

As part of this effort, TSA is proposing to move and consolidate all the requirements for security training of security-sensitive employees (currently referenced in §§ 1570.107, 1570.109, 1570.111, 1570.121, 1580.113, 1580.115, 1582.113, 1582.115, and 1584.113, and 1584.115) into one section in each of the modal-specific parts (proposed §§ 1580.113, 1582.113, and 1584.113) rather than the current structure, which has some requirements in part 1570 and some in multiple sections in parts 1580, 1582, and 1584. None of the requirements for security training (procedural or substantive) would be modified through this rulemaking.

Finally, TSA is proposing to require the pipeline facilities and systems within the applicability of the CRM program requirements (proposed § 1586.101(b)) to designate a Physical Security Coordinator and report significant physical security concerns. For almost a decade, TSA's Pipeline Guidelines have encouraged pipeline owner/operators to

[192] This requirement is consistent with sections 1512(e)(2) and 1531(e)(2) of the 9/11 Act, as codified at 6 U.S.C. 1162(e)(2) and 1181(e)(2), respectively.

report security incidents to TSA[193] and provide contact information for security operations or controls centers for pipeline owner/operators in order to facilitate the exchange of information.[194] Through this rulemaking, TSA is proposing to make having a Physical Security Coordinator and reporting significant physical security concerns mandatory for the pipeline owner/operators identified in proposed § 1586.101(b). Expanding these requirements to this critical sector would ensure TSA is able to obtain a complete picture of potential threats, both physical and cyber across this sector and as it relates to other critical infrastructure.

F. General procedures for security programs, SDs, and Information Circulars

1. General procedures for security programs (proposed revisions to subpart B of part 1570)

In the Security Training for Surface Transportation Employees final rule, TSA established procedures for security programs in 49 CFR part 1570. At that time, the requirements to be included in a security program were primarily related to security training. As part of this rulemaking and the expansion of security program requirements to include a robust CRM program, TSA is proposing to revise the procedures for security programs in part 1570 to align more closely with the well-established procedures applicable to security programs issued for civil aviation under subchapter C of 49 CFR chapter XII. In general, these changes primarily result in reorganizing the requirements currently in §§ 1570.109 through 1570.119.[195] In addition, these procedures also address allowances in the 9/11 Act for coordinated development and implementation of vulnerability assessments and security plans, and the requirements in the 9/11 Act related

---

[193] *See supra* note 81, at Appendix B.
[194] *See* Supporting Statement for OMB Control No. 1652-0055, as approved on Dec. 22, 2010, available at https://www.reginfo.gov/public/do/PRAViewICR?ref_nbr=201006-1652-001 (last accessed Nov. 28, 2023).
[195] *See supra* at Table 3 for distribution of current requirements.

to recognition of existing procedures, protocols, and standards.[196]

Proposed § 1570.107 includes the procedures for when an owner/operator determines that they need to amend a security program previously approved by TSA. This section is consistent with the procedures for aviation security programs under subchapter C of Chapter XII[197] and would replace current §§ 1570.113 and 1570.117. These procedures ensure a joint understanding between TSA and owner/operators on what the owner/operator is committed to implementing while providing opportunities to modify measures as necessary to address changes in operations, evolving capabilities, and emerging threats. As the COIP is a security program, owner/operators must request an amendment whenever they seek to make substantive changes to their COIPs or to documents incorporated by reference. Current § 1570.113 includes requirements for when owner/operators must request an amendment to their security programs. TSA is proposing to consolidate and streamline these requirements in proposed 1570.107(c).

Proposed § 1570.107(b) includes the general requirements for owner/operators to request an amendment to a TSA-approved security program. Current § 1570.113(e) requires owner/operators to submit a request for an amendment to their programs no later than 65 days after a permanent change takes effect. For purposes of this requirement, a permanent change is any change in effect for 60 or more calendar days.[198] The SDs for cybersecurity requirements require a request for an amendment no later than 50 calendar days after the permanent change takes effect, unless TSA allows a longer time period. A permanent change for that purpose is any change intended to be in effect for 45 or more calendar days.[199] In TSA's aviation programs, TSA requires requests for amendments 45 days *before* they take effect, unless TSA allows a shorter time period.[200]

---

[196] *See* sections 1405(g), (i) and 1512(j), (l) of the 9/11 Act, as codified at 6 U.S.C. 1134(g), (i) and 1162(j), (l), respectively.
[197] *See* 49 CFR 1542.105, 1544.105, 1548.7, and 1549.7.
[198] *See* 49 CFR 1570.113(d).
[199] *See* section VI of the SD Pipeline-2021-02 and SD 1580/82-2022-01 series.
[200] *See, e.g.*, 49 CFR 1542.105(b)(1).

Under the proposed rule, permanent changes would continue to be those intended to be in effect for 60 or more days, but owner/operators would be required to request an amendment at least 45 days *before* the change takes effect. This section carries over from current § 1570.113(f), the TSA standard for approval. In general, this standard requires that the policies, procedures, or measures in the proposed amendment provide a commensurate level of security to the previously approved policy, procedure, or measure. As validated by TSA's application of this timeframe in aviation programs, this requirement benefits both the agency and owner/operator by ensuring that TSA agrees with the owner/operator's determination that a modification to previously approved procedures will continue to meet the required security objectives. This agreement, in turn, avoids situations where an owner/operator invests in programs, capabilities, or technology that TSA subsequently disapproves because the modification fails to provide adequate security as required by the regulation.

Proposed § 1570.113(c)(1) specifically excludes administrative or clerical changes from the amendment process. These changes are those that do not affect policies procedures, or measures in the owner/operator's TSA-approved security program. While an amendment is not required, TSA would require owner/operators to maintain a chronological record of these changes for at least one year before the date of the last approved security program. As with all other documentation of compliance, this information be provided to TSA upon request.

Proposed § 1570.113(c)(2) includes an exception for temporary, substantive changes. Temporary, substantive changes are those that would have an impact on approved policies, procedures, or measures, but which are not intended to be in effect for 60 or more days. For temporary, substantive changes, TSA is proposing that owner/operators must notify TSA no more than 24 hours after a temporary, substantive change is made to any policy, procedure, or measure in its TSA-approved security

program. Within 7 calendar days of this notification, the owner/operator must, in writing, inform TSA of the interim policies, procedure, or measures it is using to maintain adequate security while the temporary, substantive change is in effect. The owner/operator must include a description of how the interim policy, procedure, or measures provides a commensurate level of security. TSA will notify the owner/operator in writing if the agency does not concur that the interim measure provides a commensurate level of security. If the temporary, substantive change exceeds or is expected to exceed 60 days, then owner/operator must seek an amendment to its security program. This amendment request must be submitted no later than 65 days after the temporary, substantive change initially took effect. These proposed provisions would result in TSA having more visibility into temporary, substantive changes (consistent with TSA's regulatory requirements in the aviation context) while maintaining some of the flexibility contained in current regulations and SDs with respect to non-permanent changes. Proposed § 1570.107(c) also provides more specific detail on the difference between administrative or clerical changes and substantive revisions and the procedures to be followed based on the type of amendment.

As specifically applied to the security training programs required by §§ 1580.113, 1582.113, and 1584.113, which are also considered TSA-approved security programs, TSA notes that most revisions to a security training program would be considered substantive and permanent. Training curriculums and programs are usually planned in advance and do not change as rapidly as cybersecurity issues. Within this context, however, TSA would consider changes to the number of employees to be trained within each of the identified functions to be an administrative or clerical change, which would not require an amendment. TSA believes it is more important for the owner/operator to have an accurate and up-to-date awareness of these issues and plan accordingly than to impede this process by imposing an amendment process every time staff levels change.

As applied to the CRM program, examples of administrative or clerical, temporary, and permanent changes are discussed more fully in Section III.D.2.a., within the general context of COIP requirements.

Proposed § 1570.107(d) and (e) includes procedures for TSA to amend security programs, which align with what is currently in § 1570.115. This section also proposes to add the process for filing a petition for reconsideration, currently in § 1570.119, as proposed § 1570.107(f).

Proposed § 1570.109 provides an option for owner/operators who may have operations that meet the criteria for applicability, but those operations are infrequent or seasonal. TSA is proposing to add a section that aligns with an option provided to airports in 49 CFR 1542.109. Under this provision, TSA may make a risk-based determination to impose alternative requirements that are appropriate for the scope of the operations rather than the full programmatic requirements.

TSA is proposing to add § 1570.115, which provides the procedures for withdrawing approval of a security program. In general, if an owner/operator is not in compliance with regulatory requirements, TSA would work through an enforcement process that has a range of actions including notices and an opportunity to correct and penalties. In some situations, however, TSA may determine that the failure to comply is so contrary to security and the public interest that the agency must withdraw approval of the security program. Section 1570.115 provides the standard and process for withdrawal to ensure due process is provided should this action be necessary.

In proposed § 1570.117, TSA would incorporate the general recordkeeping requirements from current § 1570.121. The recordkeeping requirements specific to physical security training have been incorporated into the proposed consolidated physical security training requirements in the modal-specific parts, specifically in proposed §§ 1580.113, 1582.113, and 1584.113.

Finally, as part of the general effort to establish comprehensive regulatory regime for surface regulations similar to the regime for aviation, TSA is proposing to revise § 1570.1 to add paragraph (b). This paragraph clarifies that the authority for any function exercised by the Administrator within the subchapter, such as approving an amendment to a security program, may be delegated to other officials by the Administrator. The statement is consistent with current 49 CFR 1540.3, as applied to aviation, and is appropriate as TSA continues to implement its authority and responsibilities for surface transportation security.

2. SDs and Information Circulars (proposed subpart C of part 1570)

TSA is also proposing to rename Subpart C – Operations to Subpart C –Threat and Threat Response and add a new § 1570.201 related to the issuance of SDs and ICs.[201] This section would provide procedures in TSA's regulations to issue SDs and ICs and make other revisions to align TSA's processes for surface transportation security with those long-established for the aviation sector.

The surface cybersecurity SDs discussed in section II.B.1. were issued under the authority of 49 U.S.C. 114(*l*)(2). Aviation SDs, however, are a creature of APA rulemaking, having been created by the Federal Aviation Administration (FAA).[202] When TSA determines that it must immediately require additional security measures to respond to a threat assessment or to a specific threat against civil aviation, it may issue SDs to certain regulated parties. Regulated parties may request alternative procedures to accomplish the same security goal with different measures.[203] Unless otherwise

---

[201] As discussed above, TSA proposes to move existing sections 1570.201 and .203 to parts 1580, 1582 and 1584.

[202] *See* 54 FR 28984 (July 10, 1989); 58 FR 36802 (July 8, 1993) (aircraft operators); 66 FR 37274 (July 17, 2001) (airport operators). Requirements are now in 49 CFR 1542.303 (airport operators) and 1544.305 (aircraft operators). The FAA's transportation security authority and all rules were given to TSA under ATSA. *See* 49 U.S.C. 114(d); section 141 of ATSA (Savings Provision). As a result, Aviation SDs are not issued under 49 U.S.C. 114 (*l*)(2).

[203] *See* 49 CFR 1542.303 (airport operators); 1544.305 (aircraft operators); 1548.19 (indirect air carriers); and 1549.109 (Certifier Cargo Screening Facilities). The foreign air carrier regulations in 49 CFR part 1546 do not provide for SDs. TSA issues emergency amendments (EAs) to their security programs to require additional security measures when needed.

determined by the Administrator, SDs contain SSI and thus are not available to the general public.[204] Review of an SD is available in a U.S. court of appeals.[205]

The provisions for SD procedures also address issuance of ICs. ICs are intended to notify owner/operators of specific security concerns and may include recommended measures to address the concern. While a specific regulatory provision is not necessary to issue ICs, referencing them in the regulations provides a distinction between voluntary versus mandatory measures.

Through this rulemaking, TSA is proposing to create a similar regulatory provision for SDs and ICs for surface transportation to those applicable in the aviation sector.[206] As discussed above, *see* section II.B.1 of this NPRM, TSA has used these two types of actions to address cybersecurity of surface transportation. TSA made a risk-based decision that certain entities must implement cybersecurity measures. Those entities were within the scope of applicability for the SDs. TSA also issued ICs to all owner/operators within a certain mode, recommending that they consider voluntarily implementing the measures imposed on the higher-risk owner/operators. ICs are distinguished from more general guidance documents because they are specific to a certain security concern. This addition to TSA's regulations would ensure that any person within the scope of applicability of future SDs or ICs would be able to find the applicable procedures for these actions in TSA's regulations.

As noted above, TSA is proposing revisions to streamline regulatory text for owner/operators to request to implement security measures other than those specifically required by TSA, or to revise previously approved security programs. The current regulations provide for amendments to security programs requested by an owner/operator

---

[204] *See* 49 CFR 1520.5(b)(2) regarding SDs.
[205] *See Gilmore v. Gonzales,* 435 F.3d 1125, 1133 (9th Cir. 2006) (which held that SDs are an agency order subject to court of appeals review pursuant to 49 U.S.C. 46110); *see also Corbett v. Transp. Sec. Admin.*, 19 F4th 478, 480 (D.C. Cir. 2021).
[206] *See* 49 CFR 1542.303, 1544.305, 1548.19, and 1549.109.

in current 49 CFR 1570.113, TSA amendments to programs in § 1570.115, and owner/operator requested alternative procedures in § 1570.117. Under the current regulations, the distinction between an owner/operator amendment and an alternative procedure is not clear as they both authorize the owner/operator to request to implement a measure other than what is required by TSA and require TSA to determine that granting the request would not have a negative impact on security.

TSA is also proposing to revise the procedures for amendments to security programs (such as the COIP) required by subchapter D. *See* discussion in section II.F.1. As part of this revision, TSA is proposing to move the procedures for requesting alternative measures from current § 1570.117 to § 1570.203, and to limit the alternative procedures measures to SDs. This revision would provide owner/operators with a clearly identified process for requesting to implement alternatives to requirements in an SD. The proposed procedures align with our standard processes for aviation where we require owner/operators to request an amendment to a security program through the security program process, and also allow owner/operators the ability to request an alternative measure or procedure to requirements in an SD. Owner/operators would continue to be able to request amendments to their security programs under proposed § 1570.107(b).

3. Exhaustion of administrative remedies (proposed § 1570.119)

TSA is proposing to add a new § 1570.119, which would require exhaustion of administrative remedies before challenging final agency orders by TSA related to the requirements in parts 1570, 1580, 1582, 1584, and 1586. Under this proposed requirement, an individual could not seek judicial review until TSA has issued its "final agency order." TSA has identified in proposed subpart B of part 1570 the point at which a TSA decision is a "final agency action." For purposes of this rulemaking, "final agency order" and "final agency action" have the same meaning.

This requirement would apply to (a) denials of approval of a security program or

an amendment to a security program, alternative measures to requirements in a security program; (b) imposition of requirements through an SD or TSA-required amendment to a security program; and (3) withdrawal of a security program. For example, if the specific regulatory provision provides for an owner/operator to request a petition for reconsideration of a denial of security program amendment, *see* proposed § 1570.107(f), then the owner/operator would need to have a timely petition for reconsideration denied before they would have exhausted the administrative procedures.

The doctrine of exhaustion of administrative remedies is based on the need to conserve judicial resources and ensure that factual issues are resolved by the agency with the expertise and responsibility for administering the program at issue. The doctrine allows agencies to develop a full factual record, correct errors, minimize costs, and create a uniform approach to the issues within its jurisdiction. This process benefits individuals by resolving disputes more quickly and at lower cost through TSA rather than the federal courts. If the individual ultimately seeks review in the Court of Appeals following TSA's final agency order, the court would have a full record on which to base its review, and the issues would be narrowed to those that truly require judicial review.[207] This process also allows TSA the opportunity to correct any errors and narrow the issues, which can be achieved through exhausting administrative remedies, before initiating judicial review.[208]

For all of the foregoing reasons, TSA is proposing to include in the regulation an explicit requirement for individuals to exhaust administrative remedies before seeking judicial review.

4. Severability

Proposed § 1570.121 would reflect TSA's intent that the various regulatory

---

[207] *See Mohamed Al Seraji v. Gowadia*, No. 8:16-cv-01637-JLS-JCG (C.D. Cal. Apr. 28, 2017). In this case, TSA issued a preliminary denial of a TWIC application, and the individual sought review by a U.S. District Court rather than first appealing the decision to TSA. The court dismissed his claim, stating that he must first exhaust the administrative remedies in TSA's redress regulations. The court stated that it needed a more developed factual record to effectively evaluate the case.

[208] *Id.*

provisions be considered severable from each other to the greatest extent possible. For instance, if a court of competent jurisdiction were to hold that the rule or a portion thereof may not be applied to a particular owner or operator or in a particular circumstance, TSA would intend for the court to leave the remainder of the rule in place with respect to all other covered persons and circumstances. The inclusion of a severability clause would not be intended to imply a position on severability in other TSA regulations.

5. Enforcement and compliance

TSA has broad authority to: (1) enforce its rules and requirements; (2) oversee the implementation and ensure the adequacy of security measures; and (3) inspect, maintain, and test security facilities, equipment, and systems for all modes of transportation.[209] TSA's authority over transportation security is comprehensive and supported with specific powers related to the development and enforcement of security-related regulations and other requirements. Within this broad authority, the agency may assess a security risk for any mode of transportation and develop security measures for dealing with this risk.[210] If TSA identifies noncompliance with its requirements, TSA may hold the owner/operators responsible for the violation and subject to enforcement action, which may result in civil monetary penalties.[211] Pursuant to its statutory authority and responsibilities, TSA is the sole Federal agency with authority to enforce its regulations.

Through a separate rulemaking, TSA recently consolidated all of its provisions previously found throughout its regulations relating to inspections, including the regulations governing surface transportation entities in current 49 CFR 1570.9.[212] As a result of this revision to TSA's regulations, TSA's inspection requirements are now located in one section, 49 CFR 1503.207, which is the part that specifically focuses on

---

[209] *See generally* 49 U.S.C. 114.
[210] 49 U.S.C. 114(f) and (*l*).
[211] 49 U.S.C. 114(f) and (u).
[212] *See* Final Rule, Flight Training Security Program, 89 FR 35580 (May 1, 2024). These changes took effect on July 30, 2024.

investigative and enforcement procedures applicable to all of TSA's regulatory requirements.

When appropriate, TSA will coordinate with an owner/operator on inspections. Notice gives the parties to be inspected the opportunity to gather evidence of compliance and to arrange to have the appropriate personnel available to assist TSA. Some inspections, however, can only be effective if TSA's presence is unannounced. TSA must have the flexibility to respond to information, operations, and specific circumstances whenever they exist or develop.

Security concerns are different at different times of the day and on different days. Terrorists may seek to take advantage of vulnerabilities whenever they occur. TSA has the authority to assess the security of transportation entities at all times (including nights, weekends, and holidays) and under all operational situations. The nature of any given TSA inspection will depend on the specific circumstances surrounding a particular owner/operator at a given point in time and will be considered in conjunction with available threat information.

G. Summary of applicability and requirements

Table 6 identifies the current and proposed applicability of all the requirements discussed above.

TABLE 6: SUMMARY OF PROPOSED REQUIREMENTS

[Current subchapter D of 49 CFR chapter XII requirements are indicated with an "X"; proposed requirements are indicated with a "P"]

	SD and IC Proce-dures	Physical Security Coordi-nator	Reporting Significant Physical Security Concerns	Security Training	Cyber-security Coordi-nator	Reporting Cyber-security Incidents	CRM program
Owner/operators of freight railroads operating on general railroad system.....	P	X	X	X	P	P	P*I
Rail hazardous materials shippers.....	P	X	X	----------	----------	----------	----------

Rail hazardous materials receivers in HTUAs……	P	X	X	----------	----------	----------	----------
Owner/operators hosting freight or passenger rail operations……	P	X	X	X	P*	P*	P*
Owner/operators of private rail cars and circus trains.....	P	X**	X	----------	P**	P	----------
Owner/operators of passenger railroads operating on the general railroad system, including intercity passenger train service, and commuter train services…….	P	X	X	X	P	P	P*
Owner/operators of rail transit systems not part of general railroad system…….. .	P	X	X	X	P	P	P*
Owner/operators of tourist, scenic, historic, and excursion railroads……	P	X**	X	----------	P**	P	----------
Owner/operators of bus transit or commuter bus systems in designated areas……	P	X	X	X	----------	P	----------
OTRB owner/ operators providing fixed-route service in designated areas……	P	X	X	X	----------	P	----------
Owner/operators of pipeline facilities and systems…….	P	P*	P*	----------	P*	P*	P*

*If described in proposed 1580.301, 1582.201, or 1586.101.
**If notified by TSA in writing that a threat exists concerning that operation.

As further discussed below, this proposed rule builds upon the previously issued SDs that many of the affected owner/operators have endeavored to implement. All the

requirements in the SDs discussed in section II.B.1 of this NPRM have been carried over into the proposed rule, either in full or with minor alteration. New requirements include cybersecurity incident reporting for the OTRB industry; specific requirements for governance of the owner/operators' CRM programs; supply chain risk management requirements addressed as part of the COIP; and cybersecurity training. TSA is also proposing to include physical security requirements for the covered pipeline industry, but these provisions are not considered part of the CRM program. A summary of key updates is listed below, and a more comprehensive presentation can be found in Appendix A of the Regulatory Impact Analysis available in the docket for this rulemaking.

- Cybersecurity Evaluation (§§ 1580.305, 1582.205, and 1586.205) – The proposed requirements for a Cybersecurity Evaluation modify the assessments required by the SD Pipeline 2021-01, SD 1580-21-01, and SD 1582-21-01 series by making the requirement more comprehensive, including the development of an enterprise-wide cybersecurity profile that as set forth in the proposed rule must be updated annually. As discussed in section III.D.1, this type of evaluation is consistent with the NIST CSF. The process to develop this profile is substantively similar to the requirements laid out in the applicable SDs. This requirement also addresses certain requirements in the 9/11 Act related to vulnerability assessments.
- Cybersecurity Operational Implementation Plan (COIP) (§§ 1580.303, 1582.203, and 1586.203) – The proposed requirements for a COIP build on the requirement in the SD Pipeline-2021-02 and SD 1580/82-2022-01 series, which required covered owner/operators to develop a CIP. This requirement also addresses certain requirements in the 9/11 Act related to developing a security plan to address vulnerabilities and ensure security of certain IT and OT systems. The additional requirements in the proposed rule for the COIP are consistent with the

transition from the temporary purpose of the SDs' requirements to establishing a permanent, robust, and mature CRM program. The new proposed COIP requirements include requiring owner/operators to have a POAM, which supports prioritization and timely implementation of CRM requirements and involves owner/operators developing a plan to address any shortfalls in being able to meet the requirements of the COIP.

- Governance (§§ 1580.309, 1582.209, and 1586.209) – Consistent with TSA's intent to align the requirements in the rulemaking with the NIST CSF, TSA is proposing additional structure around the governance of the CRM program that was not included in the SDs. Establishing strong governance is critical of a viable and mature CRM program because having processes and identifying roles creates a more effective and efficient operation that considers cybersecurity and protects organizational goals. The "governance" requirements include designation of the accountable executive as well as those with cybersecurity responsibilities to have a single leader (by role/position/title) that will act as the person responsible and accountable for planning, resourcing, and execution of cybersecurity activities.
- Cybersecurity Coordinator (§§ 1580.311, 1582.211, and 1586.211) – TSA is proposing to incorporate the requirements to designate a Cybersecurity Coordinator first imposed in the SD Pipeline 2021-01, SD 1580-21-01, and SD 1582-21-01 series with a few changes that detail the knowledge and skills of the Cybersecurity Coordinator. Such areas include general cybersecurity guidance and best practices; relevant law and regulations pertaining to cybersecurity; handling of SSI and security-related communications; current cybersecurity threats applicable to the owner/operator's operations and systems as well as having a HSIN account or other TSA-designated communication platform for information sharing. The Cybersecurity Coordinator information must also be

added to the owner/operator's COIP. This requirement also addresses certain requirements in the 9/11 Act related to security coordinators, as well as recognizing the distinction between physical security and cybersecurity and the possibility that larger organizations may need to have different individuals handling these responsibilities.

- Identification of Critical Cyber Systems (§§ 1580.313, 1582.211, and 1586.211) – The proposed rule incorporates the requirement to identify Critical Cyber Systems first imposed in the SD Pipeline-2021-02 and SD 1580/82-2022-01 series that are substantively the same but contain clarifying language modifications with regards to the specifics of what is involved in the identification process. This requirement also addresses certain requirements in the 9/11 Act related to identification of critical assets and infrastructure.
- Supply Chain Risk Management (§§ 1580.315, 1582.215, and 1586.215) – TSA is proposing a new requirement, supply chain risk management, which is not in the SDs to align the CRM program requirements with CISA's CPGs. Under this requirement, the owner/operator must incorporate policies, procedures, and capabilities to address supply chain cyber vulnerabilities into their COIP.
- Protection of Critical Cyber Systems (§§ 1580.317, 1582,217, and 1586.217) – These proposed requirements incorporate requirements from the SD Pipeline-2021-02 and SD 1580/82-2022-01 series involving measures to provide network segmentation, access control, as well as patching and software updates and adds a discussion on procedures related to logging. TSA is not changing the substance but proposing to organize the requirements from the SDs to align with the NIST CSF. This requirement also helps address the 9/11 Act's requirements related to protection of certain IT and OT systems.
- Cybersecurity Training (§§ 1580.319, 1582.219, and 1586.219) – TSA is

proposing a new requirement for cybersecurity training, for basic users as well as role-based cybersecurity training for privileged users. As discussed in Section III. D.2.d., this proposed requirement is consistent with recommendations in CISA's CPGS. This requirement also addresses portions of the 9/11 Act requirements related to requiring security training for certain employees.

- Detection of Cybersecurity Incidents (§§ 1580.321, 1582.321, and 1586.321) – TSA is proposing to include requirements from the SD Pipeline-2021-02 and SD 1580/82-2022-01 series that address detection and monitoring of Critical Cyber Systems. TSA is not changing the substance but proposing to organize the requirements from the SDs to align with the NIST CSF. This proposed requirement also helps address 9/11 Act requirements related to plans to respond to a terrorist attack, which would include a cybersecurity incident caused by a threat actor.
- Capabilities to Respond to a Cybersecurity Incident (§§ 1580.323, 1582.223, and 1586.223) – This proposed requirement is included in the SD Pipeline-2021-02 and SD 1580/82-2022-01 series and involves auditing of unauthorized access to internet domains and communication between OT systems and external systems. TSA is not changing the substance but proposing to organize the requirements from the SDs to align with the NIST CSF. This proposed requirement also helps address 9/11 Act requirements related to plans to respond to a terrorist attack, which would include a cybersecurity incident caused by a threat actor.
- Cybersecurity Incident Reporting (§§ 1580.325, 1582.225, 1584.107, and 1586.225) – The proposed rule incorporates the requirement to report cybersecurity incidents first imposed in the SD Pipeline-2021-02 and SD 1580/82-2022-01 series with no changes.
- Cybersecurity Incident Response Plan (CIRP) (§§ 1580.327, 1582.227, and

1586.227) – The proposed requirement for a CIRP is incorporated from the SD Pipeline-2021-02 and SD 1580-21-01, and SD 1582-21-01 series. This proposed requirement involves having a plan to respond to cybersecurity incidents. The plan must include exercises. The CIRP requirements in the proposed rule are substantively the same as in the SDs with some language changes. This proposed requirement also helps address 9/11 Act requirements related to plans to respond to a terrorist attack, which would include a cybersecurity incident caused by a threat actor.

- Cybersecurity Assessment Plan (CAP) (§§ 1580.329, 1582.229, and 1586.229) – This proposed requirement is incorporated from the SD Pipeline-2021-02 and SD 1580/82-2022-01 series with no substantive changes and involves a robust assessment plan that tests the effectiveness of the COIP. As laid out in the applicable SDs, consistent with the NIST CSF, the proposed requirements include providing an annual report of assessment findings to TSA and corporate leadership, which feeds into the iterative cycle of assessments, planning, implementation, testing, and revisions to plans, that is critical to having a meaningful CRM program.

H. Compliance deadlines and documentation

Table 7 identifies compliance deadlines and the type of documentation required to meet compliance requirements.

TABLE 7: COMPLIANCE DEADLINES AND DOCUMENTATION

Requirement	Record Mechanism	Deadlines	Source	Amendment Required for Substantive Changes
Cybersecurity Evaluation	Owner/operator holds for inspection	Completed no later than 90 days after effective date of final rule or 45 days before commencing new or modified operations (but no more than one year before date of submission of	1580.305(b), 1582.205(b), and 1586.205(b)	No

		COIP).		
		Must notify TSA within 7 days of completion.	1580.305(d), 1582.205(d), and1586.205(d)	---
		Annual updates required.	1580.305(c), 1582.205(c), and1586.205(c)	---
COIP	Submitted to TSA for review and approval	No later than 180 days after effective date of final rule or 45 days before commencing new or modified operations.	1580.307(e),1582.207(e), and 1586.207(e)	*See* below for individual requirements
		Must be reviewed and updated within 60 days of completed Cybersecurity Evaluation or CAP Report.	1580.307(f), 1582.207(f), and 1586.207(f)	---
Identification of accountable executive and individuals/vendors with cybersecurity responsibilities	Included in COIP	Notification to TSA within 30 days of effective date of final rule and within 7 days of changes to previously submitted information.	1580.309(a), 1582.209(a), and 1586.209(a)	No; but notification to TSA if changed
Designation of Cybersecurity Coordinator	Notification to TSA; information included in COIP	Notification to TSA within 7 days of effective date of final rule (if not previously provided) and within 7 days of changes to previously submitted information that occur after that date.	1580.313(d), 1582.213(d), and 1586.213(d)	No; but notification to TSA if changed
Identification of Critical Cyber Systems and Network Architecture	Included in COIP	No separate deadline from COIP submission.	---	Yes
Supply Chain Risk Management	Included in COIP	No separate deadline from COIP submission.	---	Yes
Description of how protective security outcomes are met	Included in COIP	No separate deadline from COIP submission.	---	Yes
Cybersecurity training	Included in COIP	Initial training within 60 days of approval of COIP or 10 days of onboarding.	1580.319(d), 1582.219(d), and 1586.219(d)	Yes
		Annual training 1 year from employee's last training.	1580.319(e), 1582.219(e), and 1586.210(e)	---
Description of how detection and monitoring security outcomes are met	Included in COIP	No separate deadline from COIP.	---	Yes

Cybersecurity Incident Reporting	Notification to CISA	Within 24 hours of identification.	1580.325(a), 1582.225(a), and 1584.107(a), and 1586.225(a)	No
Description of how response security outcomes are met	Included in COIP	No separate deadline from COIP.	---	Yes
CIRP	Included in COIP	No separate deadline from COIP, but notification within 15 days if CIRP previously submitted as part of COIP is modified.	1580.329(f), 1580.229(f), and 1586.229(f)	No; but notification to TSA if changed
POAM	Included in COIP	No separate deadline from COIP (target dates cannot extend beyond three years from date of submission of COIP for TSA approval).		Yes
CAP	Submitted to TSA for review and approval	No later than 90 days from approval of COIP.	1580.329(a), 1582.229(a), and 1586.229(a)	No
		Report submitted 15 months from TSA approval of CAP and annually thereafter.	1580.329(e), 1582.229(e), and 1586.229(e)	---
		Annual update to CAP, submitted no later than 12 months from date of last TSA-approval of CAP.	1580.329(f), 1582.229(f), and 1586.229(f)	---

I. Sensitive Security Information

1. Scope of the revision to TSA's SSI regulatory requirements

TSA is proposing minor changes to 49 CFR part 1520. These revisions consist of two types of modifications. First, revisions ensure the scope of existing designations of SSI for SDs and information circulars includes the section that would be added through this rulemaking as applicable to surface transportation. Second, TSA identified several areas where the SSI regulations explicitly referencing aviation and maritime should be revised to include surface transportation because similar requirements for surface transportation did not exist when the SSI regulations were promulgated. This proposed rule would address that gap.

Note that any security program, security plan, or contingency plan required by 49

CFR subchapter D and vulnerability assessments required by, or submitted to TSA, are designated as SSI under current § 1520.5(b)(1) and (5), respectively. These requirements remain subject to SSI protection except as otherwise provided in writing by TSA in the interest of public safety or in furtherance of transportation security.[213]

2. Disclosure of SSI upon the "need to know"

Each owner/operator subject to the requirements in this proposed rule is a covered person under 49 CFR 1520.7(n) and is, therefore, required to protect SSI from unauthorized disclosure. TSA's SSI requirements do not prohibit owner/operators from sharing SSI with specific vendors that have a "need to know." Determining whether information can be shared is a two-step consideration. First, is the individual a "covered person" under 49 CFR 1520.7. Under § 1520.7(k), employees and contractors of an owner/operator are "covered persons."

Section 1520.9 requires all covered persons to protect SSI from unauthorized disclosure. Before sharing information with any person employed by, contracted to, or acting for a covered person, § 1520.9(a)(2) requires the owner/operator to determine that the individual has a need to know the information or record designated as SSI, as described in § 1520.11. If the person has a need to know and the information is shared, that individual is a covered person who is required to protect SSI from unauthorized disclosure.[214] When providing the SSI, the owner/operators must include the SSI protection requirements and ensure the covered person is formally advised of their regulatory requirements to protect the information. The materials provided must maintain their SSI markings and be accompanied with an SSI cover sheet, and SSI must be properly disposed of in accordance with TSA regulations.[215]

---

[213] *See* 49 CFR 1520.5(c) for TSA determinations that information no longer constitutes SSI.
[214] *See* 49 CFR 1520.7(j), 1520.7(k) and 1520.9.
[215] *See* 49 CFR 1520.9, 1520.13, and 1520.19 for specific restrictions related to restrictions on disclosure, marking, and destruction of SSI, respectively.

Unauthorized disclosure of SSI, by owner/operators or their vendors, is grounds for enforcement action by TSA, including civil penalty actions, under § 1520.17. To support compliance with these requirements, TSA provides resources to regulated entities and other person on proper handling of SSI.[216]

IV. Regulatory Analyses

A. Economic Impact Analysis

1. Summary of Regulatory Impact Analysis

Changes to federal regulations must undergo several economic analyses. First, E.O. 12866 of September 30, 1993 (Regulatory Planning and Review),[217] as supplemented by E.O. 13563 of January 18, 2011 (Improving Regulation and Regulatory Review),[218] and amended by E.O. 14094 of April 6, 2023 (Modernizing Regulatory Review)[219] directs Federal agencies to propose or adopt a regulation only upon a reasoned determination that the benefits of the intended regulation justify its costs. Second, the Regulatory Flexibility Act of 1980 (RFA)[220] requires agencies to consider the economic impact of regulatory changes on small entities. Third, the Trade Agreement Act of 1979[221] prohibits agencies from setting standards that create unnecessary obstacles to the foreign commerce of the United States. Fourth, the Unfunded Mandates Reform Act of 1995 (UMRA)[222] requires agencies to prepare a written assessment of the costs, benefits, and other effects of proposed or final rulemakings that include a federal mandate likely to result in the expenditure by State, Local, or Tribal governments, in the aggregate, or by the private sector, of $100 million or more annually ($177 million

---

[216] *See* SSI Best Practices Guide for Non-DHS Employees or contact TSA at (571) 227-3513 or SSI@tsa.dhs.gov. Additional resources are available at https://www.tsa.gov/for-industry/sensitive-security-information (last accessed Sept. 24, 2023).
[217] Published at 58 FR 51735 (Oct. 4, 1993).
[218] Published at 76 FR 3821 (Jan. 21, 2011).
[219] Published at 88 FR 21879 (Apr. 6, 2023).
[220] Public Law 96–354. 94 Stat. 1164 (Sept. 19, 1980), as codified at 5 U.S.C. 601 *et seq.,* as amended by the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA).
[221] Public Law 96–39, 93 Stat. 144 (July 26, 1979), as codified at 19 U.S.C. 2531–2533.
[222] Public Law 104–4, 109 Stat. 66 (Mar. 22, 1995), as codified at 2 U.S.C. 1181–1538.

adjusted for inflation).[223]

The security of the nation's transportation systems is vital to the economic health and security of the United States. Surface transportation systems in particular—including public transportation systems, intercity and commuter passenger railroads, freight railroads, intercity buses, hazardous liquid and liquefied natural gas pipelines as well as natural gas pipelines, and related infrastructure—are vital to our economy and essential to national security.[224]

As discussed previously in this preamble, threat actors have demonstrated their willingness to engage in cyber intrusions and perpetrate cybersecurity incidents against critical infrastructure. As technology evolves, so do cybersecurity threats. A successful attack could result in significant negative consequences with potential cascading impacts across many sectors of the economy and people's lives.

Transportation companies have competing priorities with finite resources in which to confront the complexity of building a cybersecurity defense. At the same time, there is a level of uncertainty associated with being impacted by cybersecurity incidents. These competing priorities and level of uncertainty leads to a less than socially optimal level of cybersecurity investment.[225] If entities are required to implement the same requirements, there could be fewer free riders or undercutting of cybersecurity investment in favor of profits or due to budgetary constraints. As noted in the National Cybersecurity Strategy,

> Today's marketplace insufficiently rewards—and often disadvantages—the owners and operators of critical infrastructure who invest in proactive measures to prevent or mitigate the effects of cybersecurity incidents. Regulation can level the playing field, enabling healthy competition without sacrificing cybersecurity or operational resilience.[226]

Ensuring transportation security while promoting the movement of legitimate travelers and commerce is a critical mission assigned to TSA. TSA believes this proposed rule is consistent with its mission given the heightened risk of a cybersecurity threat and the potential of threat actors targeting the transportation system with the purpose to disrupt the supply chain, jeopardize public safety, undermine confidence in the transportation system, and otherwise affect national and economic security.

The primary benefit of this proposed rule is a potential reduction in the risk of successful cybersecurity incidents as well as the impact of such incidents on the public, economy, and national security. The proposed requirements could enhance the security of the regulated population, which would reduce the chance of negative consequences and service interruptions from cybersecurity incidents for surface modes like freight railroad, passenger railroad, and pipelines, thereby benefiting owners/operators, passengers, and consumers. A break-even analysis suggests that the prevention of a few significant cybersecurity incidents or a high-consequence incident in any transportation mode provides benefits in excess to the costs of the proposed rule on those modes.

---

[223] $100 million in 1995 dollars adjusted for inflation to 2022 using the GDP implicit price deflator for the U.S. economy. Federal Reserve Bank of St. Louis. "GDP Implicit Price Deflator in United States." Available at: https://fred.stlouisfed.org/series/USAGDPDEFAISMEI#0 (last accessed Sept. 30, 2023).
[224] Surface Transportation and Rail Security Act of 2007, Report of the Senate Committee on Commerce, Science, and Transportation, S. Rep. No. 110-29, at 2 (quoting Exec. Order No. 13416 (Dec. 5, 2006), available at https://www.govinfo.gov/content/pkg/CRPT-110srpt29/html/CRPT-110srpt29.htm.
[225] *See Cybersecurity* trends: Looking over the horizon (Mar. 10, 2022), available at https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-trends-looking-over-the-horizon (last accessed July 25, 2024).
[226] *Supra* note 12 at 8-9.

TSA estimates the preliminary 10-year total costs of the proposed rule to be about $2.6 billion discounted at a 3 percent discount rate and $2.2 billion discounted at 7 percent discount rate, with preliminary annualized costs of about $307.8 million. These preliminary estimates do not consider current industry practice or compliance with recently issued SDs due of a lack of data on the existing internal security practices of individual companies. As a result, many owner/operators may already employ measures that meet the security outcomes that would be required by this proposed rule and therefore have already incurred costs, which means the cost estimate of this proposed rule could be an overestimate when measured against a no-action baseline. Furthermore, costs of implementing measures to meet the proposed security outcomes may vary greatly across modes and by each owner/operator's unique needs and scale of operation. Consequently, TSA is requesting public comment on current cybersecurity industry practices and how these practices may vary by company. TSA will consider these public comments and any data provided when estimating the cost of the final rule.

2. Assessments required by E.O.s 12866 and 13563

E.O.s 12866 and 13563 direct agencies to assess the costs and benefits of available regulatory alternatives and, if regulation is necessary, select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). Under E.O. 12866, as amended by E.O. 14094, agencies must also determine whether a regulatory action is significant.[227] These requirements were supplemented by E.O. 13563, which emphasizes

[227] *See* section 1(b) of E.O. 14094, revising section 3(f) of E.O. 12866: "Significant regulatory action" means any regulatory action that is likely to result in a rule that may: (1) have an annual effect on the economy of $200 million or more (adjusted every 3 years by the Administrator of OIRA for changes in gross domestic product); or adversely affects in a material way the economy, a sector of the economy, productivity, competition, jobs, the environment, public health or safety, or State, Local, Territorial, or Tribal governments or communities; (2) create a serious inconsistency or otherwise interfere with an action taken or planned by another agency; (3) materially alter the budgetary impact of entitlements, grants, user fees, or loan programs or the rights and obligations of recipients thereof; or (4) raises legal or policy issues for which centralized review would meaningfully further the President's priorities or the principles set forth in this Executive order, as specifically authorized in a timely manner by the Administrator of OIRA in each case.

the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. In accordance with E.O. 12866, TSA has submitted the proposal to the OMB, which has determined that this proposed rule is a "significant regulatory action" as defined under section 3(f)(1) of E.O. 12866, as amended by E.O. 14094, its annual effects on the economy would exceed $200 million in any year of the analysis. In conducting these analyses:

- TSA prepared an Initial Regulatory Flexibility Analysis (IRFA), which estimates that this rulemaking would likely have a regulatory cost that exceeds one percent of revenue for 26 small entities—17 freight rail and nine pipeline owner/operators—of the 103 small entities that TSA found would be impacted by the NPRM.
- This rulemaking would not constitute a barrier to international trade.
- Under 2 U.S.C. 1503(5), this rulemaking is not subject to UMRA review because it is a regulation necessary for the national security of the United States. As noted in the National Cybersecurity Strategy, this rulemaking is being promulgated because of national security concerns related to the protection of Critical Cyber Systems, the loss or disruption of which could have impacts on national security, including economic security.

TSA has prepared an analysis of its estimated costs and benefits, summarized in the following paragraphs, and in the OMB Circular A–4 Accounting Statement. When estimating the cost of a rulemaking, agencies typically estimate future expected costs imposed by a regulation over a period of analysis. For this rulemaking's period of analysis, TSA uses a 10-year period of analysis to estimate the initial and recurring costs to the regulated surface mode owner/operators and new owner/operators that are expected due to industry growth.

a. Costs

TSA summarizes the undiscounted costs of the proposed rule to be borne by five types of parties: freight rail owner/operators, PTPR owner/operators, OTRB owner/operators, pipeline owner/operators, and TSA. Table 8 shows the breakdown of modal entity populations over the 10-year period of analysis. The population of each industry is important because it acts as a cost multiplier for some of the proposed rule's provisions (*e.g.,* employee training). The population estimates accounts for entity growth, employee growth, and employee turnover dynamics over the period of analysis, which impact the population estimate as well as factor into various costs (*e.g.*, identification of new cybersecurity coordinators with entity growth or employee turnover). It includes entity growth, employee growth, and employee turnover.

TABLE 8: POPULATION GROWTH AND TURNOVER FOR MODAL ENTITIES

Year	Freight Rail			PTPR			OTRB	Pipelines		
	Entities	Employees		Entities	Employees		Entities	Entities	Employees	
	Growth	Growth	Turn-over	Growth	Growth	Turn-over	Growth		Growth	Turnover
	$a = (a_{Y1} - 6) \times (1 + 0.85\%)^{(Y_n - 1)} + 6$	$b = b_{Y1} \times (1+0.42\%)^{(Y_n - 1)}$	$c = b \times 4.00\%$	$d = d_{Y1} \times (1 + 2.19\%)^{(Y_n - 1)}$	$e = e_{Y1} \times (1+1.11\%)^{(Y_n - 1)}$	$f = e \times 12.96\%$	$g = g_{Y1} \times (1+2.50\%)^{(Y_n - 1)}$	h	$i = i_{Y1} \times (1+0.62\%)^{(Y_n - 1)}$	$j = i \times 13.67\%$
1	73	116,960	0	34	299,680	0	71	115	39,920	0
2	74	117,451	4,698	35	303,006	39,270	73	115	40,168	5,491
3	74	117,945	4,718	36	306,370	39,706	75	115	40,417	5,525
4	75	118,440	4,738	36	309,771	40,146	76	115	40,667	5,559
5	75	118,937	4,757	37	313,209	40,592	78	115	40,919	5,594
6	76	119,437	4,777	38	316,686	41,042	80	115	41,173	5,628
7	76	119,939	4,798	39	320,201	41,498	82	115	41,428	5,663
8	77	120,442	4,818	40	323,755	41,959	84	115	41,685	5,698
9	78	120,948	4,838	40	327,349	42,424	87	115	41,944	5,734
10	78	121,456	4,858	41	330,982	42,895	89	115	42,204	5,769

Table 9 shows the 10-year cost by regulated industry. This information includes industry's costs associated with implementing the proposed requirements. Many of the costs are based on the time to complete identified actions (*e.g.*, submitting accountable executive information). In these instances, TSA calculates an opportunity cost based on the time to complete the task, approximate wage rate of the person thought to complete

the task, and how frequently the task would need to be completed. Other costs are based on expenses incurred (*e.g.*, cost to store backup data). In both cases, these costs may change over time with a higher initial cost then lower maintenance cost later. *See* TSA CRM Preliminary Regulatory Impact Analysis (RIA) for a more detailed discussion and breakdown of the costs.

TABLE 9: TOTAL UNDISCOUNTED COST OF THE PROPOSED RULE BY REGULATED INDUSTRY ($ THOUSANDS)

Year	Cost by regulated industry				Total regulated industries cost
	Freight Rail	PTPR	OTRB	Pipelines	
	a	b	c	d	e = a + b + c + d
1	$97,652	$119,996	$188	$85,636	$303,473
2	95,471	120,633	6	81,122	297,233
3	94,622	121,508	6	79,132	295,268
4	97,003	123,883	6	82,232	303,124
5	96,187	124,814	6	80,265	301,273
6	98,675	127,289	7	83,509	309,479
7	97,885	128,279	7	81,565	307,736
8	100,405	130,821	7	84,833	316,065
9	99,648	131,874	7	82,914	314,442
10	102,200	134,484	7	86,207	322,899
Total	$979,750	$1,263,581	$248	$827,415	$3,070,993

Note: Totals may not add due to rounding.

As displayed in Table 10, TSA estimates the 10-year total cost of this proposed rule to be $3.09 billion undiscounted, $2.63 billion discounted at 3 percent, and $2.16 billion discounted at 7 percent. The costs to industry (all four surface modes) comprise approximately 99 percent of the total costs of the proposed rule; and the remaining costs are incurred by TSA. TSA calculated a total cost to each industry based on estimates and assumptions on activities entities would likely engage in to be in compliance with the requirements of the proposed rule. However, due to the scope and performance-based nature of the requirements, TSA recognizes there would be variation in costs to individual covered owner/operators. In response, TSA provides a sensitivity analysis of key cost drivers in section 3.8 of the RIA, which include access control implementation, Critical Cyber System data backups, and cybersecurity training. In addition, there are

some areas where there may be unquantified cost. For example, costs related to actual mitigation measures implemented as a result of the proposed rule that are not otherwise captured in TSA's cost estimates. TSA requests comment on any costs that have not been quantified but may occur as a result of this proposed rule.

TABLE 10: TOTAL COST OF THE PROPOSED RULE ($THOUSANDS)

Year	Total regulated industries cost	TSA cost	Total proposed rule cost		
			Undiscounted	Discounted at 3%	Discounted at 7%
	a (Table 8)	b	c = a + b		
1	$303,473	$4,426	$307,899	$298,932	$287,757
2	297,233	2,408	299,641	282,440	261,718
3	295,268	2,412	297,681	272,420	242,996
4	303,124	1,358	304,482	270,529	232,288
5	301,273	1,363	302,636	261,056	215,775
6	309,479	1,368	310,847	260,329	207,130
7	307,736	1,372	309,109	251,334	192,497
8	316,065	1,377	317,443	250,592	184,755
9	314,442	1,382	315,825	242,053	171,788
10	322,899	1,387	324,286	241,299	164,851
Total	$3,070,993	$18,854	$3,089,847	$2,630,984	$2,161,554
Annualized				$308,432	$307,757

Note: Totals may not add due to rounding.

Table 11 shows the 10-year costs for the CRM program for the freight rail, PTPR, pipelines, and TSA. TSA estimates the 10-year total cost of the CRM program to be $3.00 billion undiscounted, $2.55 billion discounted at 3 percent, and $2.10 billion discounted at 7 percent. The CRM program is the largest cost provision. These costs include the cybersecurity evaluation (CSE) (which involves an enterprise-wide CSE); the COIP (which includes items related to the Cybersecurity Coordinator, identification of critical cyber systems, supply chain risk management, protection of critical cyber systems, incident response, training, detection of incidents, and the POAM); the CAP (which involves creating and submitting a plan that assesses the effectiveness of the COIP); and recordkeeping and compliance (which relates to those items needed to show compliance with provisions of the proposed rule).

TABLE 11: TOTAL COST OF THE CRM PROGRAM ($THOUSANDS)

Year	CRM program				Total cost of the CRM program		
	CSE	COIP	CAP	Recordkeeping and compliance	e = ∑a,b,c,d		
	a	b	c	d	Undiscounted	Discounted at	Discounted at

						3%	7%
1	$1,381	$290,796	$3,175	$1,005	$296,357	$287,726	$276,970
2	1,386	280,519	8,212	1,009	291,126	274,414	254,281
3	1,390	283,494	3,242	1,013	289,139	264,604	236,024
4	1,395	285,223	8,280	1,017	295,915	262,917	225,752
5	1,400	288,308	3,312	1,022	294,041	253,642	209,647
6	1,404	291,443	8,351	1,026	302,224	253,108	201,385
7	1,409	294,636	3,383	1,030	300,458	244,300	187,110
8	1,414	297,892	8,423	1,035	308,764	243,741	179,703
9	1,419	301,202	3,457	1,039	307,117	235,380	167,051
10	1,424	304,583	8,498	1,043	315,549	234,798	160,409
Total	$14,023	$2,918,095	$58,333	$10,240	$3,000,691	$2,554,629	$2,098,332
Annualized						$299,480	$298,755

Note: Totals may not add due to rounding.

Table 12 shows the 10-year costs by requirement for the freight rail industry. TSA estimates the 10-year costs to the freight rail industry to be $980 million undiscounted.[228]

TABLE 12: REQUIREMENT COSTS - FREIGHT RAIL ($ THOUSANDS)

Year	Familiarization	CRM program				Reporting Cybersecurity Incidents	CIRP	Total cost
		CSE	COIP	CAP	Record-keeping and compliance			Undiscounted
	a	b	c	d	e	f	g	h = ∑ a,b,c,d,e,f,g
1	$242	$233	$94,081	$855	$276	$1	$1,963	$97,652
2	2	235	91,019	2,514	279	1	1,422	95,471
3	2	237	91,788	881	281	1	1,433	94,622
4	2	239	92,494	2,540	283	1	1,444	97,003
5	2	241	93,295	908	285	1	1,455	96,187
6	2	242	94,108	2,567	287	1	1,467	98,675
7	2	244	94,935	935	290	1	1,478	97,885
8	2	246	95,779	2,595	292	1	1,490	100,405
9	2	248	96,638	963	294	1	1,501	99,648
10	2	250	97,515	2,622	297	1	1,513	102,200
Total	$260	$2,416	$941,652	$17,381	$2,864	$10	$15,166	$979,750

Note: Totals may not add due to rounding.

Table 13 shows the 10-year cost to the PTPR industry by requirement. TSA

[228] Costs include those related to a Cybersecurity Coordinator, reporting cybersecurity incidents, creating a CRM program (which includes the CSE, COIP, Accountable Executive, CIRP, CAP, and training), familiarization, and the costs of compliance and recordkeeping.

estimates the 10-year costs to the PTPR industry to be $1.26 billion undiscounted.[229]

TABLE 13: REQUIREMENT COSTS - PTPR ($ THOUSANDS)

Year	Familiarization	CRM program				Reporting Cybersecurity Incidents	CIRP	Total cost
		CSE	COIP	CAP	Record-keeping and compliance			Undiscounted
	a	b	c	d	e	f	g	h = ∑ a,b,c,d,e,f,g
1	$55	$103	$118,493	$389	$84	$1	$871	$119,996
2	1	106	118,601	1,164	86	1	675	120,633
3	1	108	120,197	423	88	1	690	121,508
4	1	110	121,777	1,199	90	1	704	123,883
5	1	113	123,429	458	92	1	720	124,814
6	1	115	125,106	1,235	94	1	736	127,289
7	1	118	126,816	495	96	1	752	128,279
8	1	120	128,558	1,273	98	2	768	130,821
9	1	123	130,329	534	100	2	785	131,874
10	1	126	132,139	1,312	102	2	802	134,484
Total	$66	$1,141	$1,245,446	$8,480	$931	$14	$7,503	$1,263,581

Note: Totals may not add due to rounding.

Table 14 shows the 10-year cost by requirement for the OTRB industry. TSA estimates the 10-year costs to the OTRB industry to be $248 thousand undiscounted.

TABLE 14: REQUIREMENT COSTS - OTRB ($ THOUSANDS)

Year	Reporting Cybersecurity Incidents	Familiarization	Total cost (Undiscounted)
	A	b	e = ∑ a,b,c,d
1	$1	$187	$188
2	1	5	6
3	1	5	6
4	1	5	6
5	1	5	6
6	1	5	7
7	1	5	7
8	1	5	7
9	2	6	7
10	2	6	7
Total	$14	$234	$248

Note: Totals may not add due to rounding.

Table 15 shows the 10-year cost by requirement for all the requirements for the pipeline industry. TSA is proposing to incorporate the corresponding physical security

[229] Costs include those related to a Cybersecurity Coordinator, reporting cybersecurity incidents, creating a CRM program (which includes the CSE, COIP, Accountable Executive, CIRP, CAP, and training), familiarization, and the costs of compliance and recordkeeping.

costs into this rulemaking to align pipeline with the other covered modes (for whom physical security provisions are already required). TSA estimates the 10-year costs to the combined pipeline industry to be $827 million undiscounted.[230]

TABLE 15: REQUIREMENT COSTS - PIPELINE ($ THOUSANDS)

Year	Total physical security costs	Familiari-zation	CRM program				Reporting Cyber-security Incidents	CIRP	Total cost (Undis-counted)
			CSE	COIP	CAP	Record-keeping and compliance			
	a	b	c	d	e	f	g	h	i = ∑ a, b,c,d,e,f,g ,h
1	$37	$912	$973	$74,786	$1,359	$645	$38	$6,886	$85,636
2	21	0	973	69,415	3,959	645	38	6,072	81,122
3	21	0	973	70,024	1,359	645	38	6,072	79,132
4	21	0	973	70,525	3,959	645	38	6,072	82,232
5	21	0	973	71,157	1,359	645	38	6,072	80,265
6	21	0	973	71,801	3,959	645	38	6,072	83,509
7	21	0	973	72,457	1,359	645	38	6,072	81,565
8	21	0	973	73,125	3,959	645	38	6,072	84,833
9	21	0	973	73,806	1,359	645	38	6,072	82,914
10	21	0	973	74,500	3,959	645	38	6,072	86,207
Total	$230	$912	$9,731	$721,596	$26,590	$6,446	$378	$61,531	$827,415

Note: Totals may not add due to rounding.

Table 16 shows the 10-year cost by requirement for TSA. TSA estimates the 10-year costs to TSA to be $18.9 million undiscounted.[231]

TABLE 16: REQUIREMENT COSTS - TSA ($ THOUSANDS)

Year	Physical security	CRM program			CIRP	Total cost
		CSE	COIP	CAP		Undiscounted
	a	b	c	d	e	f = ∑a,b,c,d,e
1	$75	$72	$3,436	$572	$272	$4,426
2	75	72	1,484	576	201	2,408
3	75	72	1,485	579	201	2,412
4	75	73	427	582	201	1,358
5	75	73	427	586	202	1,363
6	75	74	428	590	202	1,368
7	75	74	428	593	202	1,372

[230] Costs include those related to a Physical Security Coordinator, reporting significant physical security concerns, Cybersecurity Coordinator, reporting cybersecurity incidents, creating a CRM program (which includes the CSE, COIP, Accountable Executive, CIRP, CAP, and training), familiarization, and the costs of compliance and recordkeeping.

[231] Costs include those related to a Physical Security Coordinator, reporting significant physical security concerns, Cybersecurity Coordinator, and the CRM program (which includes the CSE, COIP, Accountable Executive, CIRP, CAP, and training). The TSA burden would be for reviewing the CRM programs, keeping track of key personnel, and ensuring compliance with the program. TSA will incur ongoing costs with the implementation of this rulemaking.

TABLE 16: REQUIREMENT COSTS - TSA ($ THOUSANDS)

Year	Physical security	CRM program			CIRP	Total cost
		CSE	COIP	CAP		Undiscounted
	a	b	c	d	e	f = ∑a,b,c,d,e
8	75	75	429	597	202	1,377
9	75	75	429	601	202	1,382
10	75	76	430	605	202	1,387
Total	$750	$735	$9,401	$5,881	$2,088	$18,854

Note: Totals may not add due to rounding.

b. Cost Sensitivity Analysis

TSA calculates a total cost for each industry based on estimates and assumptions on activities entities would likely engage in to satisfy requirements of the proposed rule. The majority of the costs are primarily driven by access control implementation, Critical Cyber System data backups, and cybersecurity training. Employee population size, which acts as a multiplication factor, is a key contributing factor for why access control and training result in such a high-cost impact. Baseline training, for instance, has a per employee burden of 1-hour per year, but when multiplied across the population of employees covered, the result is a significant expenditure. In section 3.8 of the RIA, TSA provides a sensitivity analysis that assesses uncertainty within these key cost drivers including how owner/operators may accomplish compliance and to what extent they may already meet the proposed rule requirements through existing actions and thus provide a sense of the possible practical incremental costs of the proposed rule. None of the cost drivers tested under the sensitivity analysis apply to OTRB entities; therefore, TSA did not include OTRB in the sensitivity analysis.

Specifically, TSA evaluates cost implications associated with differing assumptions related to MFA being used for access control where 25 percent are assumed to be fully implemented and an additional 25 percent are partially implemented by affected entities, rather than not implemented at all in any affected entities. For Critical Cyber System data backups, TSA assumes 20 percent of entities would fully satisfy the proposed rule's requirement and 50 percent would partially satisfy the proposed rule's

requirement. For the last cost driver evaluated, employee training, TSA varies assumed compliance with the necessary level of training from 0 percent across industry in the primary analysis to including 20 percent fully compliant and 50 percent partially compliant. The costs resulting from varying these cost driver assumptions for each mode are depicted below.

Table 17 presents freight rail sensitivity analysis costs and compares them to the freight rail costs in the primary analysis. Based on the sensitivity assumptions for access control, data backups, and cybersecurity training, the estimated total cost to freight rail is about $655.5 million which is 33 percent ($342.2 million) less than freight rail estimated cost in the primary analysis.

TABLE 17: FREIGHT RAIL SENSITIVITY COSTS ($ THOUSANDS)

Year	Sensitivity Analysis					Total cost in primary analysis	Difference from primary analysis
	Access control	Critical Cyber System backups	Cybersecurity training	All other non-cost driver costs	Total costs under sensitivity		
	a	b	c	d	e = a + b + c + d	f	g = e - f
1	$33,149	$6,665	$4,259	$22,069	$66,142	$97,652	-$31,510
2	33,289	6,870	3,981	19,989	64,128	95,471	-31,343
3	33,428	7,081	3,998	18,492	62,999	94,622	-31,624
4	33,569	7,299	4,015	20,210	65,092	97,003	-31,910
5	33,710	7,524	4,032	18,718	63,984	96,187	-32,204
6	33,851	7,756	4,049	20,516	66,172	98,675	-32,503
7	33,993	7,995	4,066	19,023	65,078	97,885	-32,808
8	34,136	8,242	4,083	20,825	67,286	100,405	-33,120
9	34,280	8,495	4,100	19,335	66,210	99,648	-33,438
10	34,424	8,758	4,117	21,139	68,437	102,200	-33,763
Total	$337,829	$76,684	$40,701	$200,314	$655,528	$979,750	-$324,221

Note: Totals may not add due to rounding.

Table 18 presents PTPR sensitivity analysis costs and compares them to the PTPR costs in the primary analysis. Based on the sensitivity assumptions, the total cost under the sensitivity is $783.4 million which is about 38 percent ($480.2 million) less than the total cost under the primary analysis. This larger percentage decrease from the primary analysis when compared to the freight rail and pipeline modes is attributed to the larger employee population within the PTPR industry. As the access control and cybersecurity

training costs are calculated on a per employee basis, these requirements make up a greater portion of the overall cost to the PTPR industry, and therefore result in a more significant cost difference within the sensitivity analysis.

TABLE 18: PTPR SENSITIVITY COST ($ THOUSANDS)

Year	Sensitivity Analysis					Total cost in primary analysis	Difference from primary analysis
	Access control	Critical Cyber System Backups	Cybersecurity training	All other non-cost driver costs	Total costs under sensitivity		
	a	b	c	d	e = a + b + c + d	f	g = e - f
1	$55,437	$3,104	$6,629	$9,433	$74,603	$119,996	-$45,394
2	56,053	3,243	6,588	8,936	74,820	120,633	-45,813
3	56,675	3,391	6,661	8,368	75,095	121,508	-46,412
4	57,304	3,544	6,735	9,279	76,861	123,883	-47,021
5	57,940	3,704	6,810	8,717	77,171	124,814	-47,643
6	58,583	3,872	6,886	9,674	79,014	127,289	-48,274
7	59,233	4,047	6,962	9,119	79,361	128,279	-48,918
8	59,891	4,230	7,040	10,086	81,247	130,821	-49,574
9	60,556	4,421	7,118	9,538	81,632	131,874	-50,242
10	61,228	4,621	7,197	10,515	83,561	134,484	-50,923
Total	$582,900	$38,176	$68,626	$93,664	$783,367	$1,263,581	-$480,214

Note: Totals may not add due to rounding.

Table 19 presents pipeline sensitivity analysis costs and compares them to the pipeline costs in the primary analysis. Based on the sensitivity assumptions, the total sensitivity analysis cost to pipeline entities is $621.7 million which is about 25 percent ($205.7) less than the primary analysis estimates. This smaller percentage decrease from the primary analysis when compared to the other modes is attributed to the smaller employee population within the pipeline industry.

TABLE 19: PIPELINE SENSITIVITY COSTS ($ THOUSANDS)

Year	Sensitivity Analysis					Total cost in primary analysis	Difference from primary analysis
	Access control	Critical Cyber System Backups	Cybersecurity training	All other non-cost driver costs	Total costs under sensitivity		
	a	b	c	d	e = a + b + c + d	f	g = e - f
1	$14,201	$10,494	$1,902	$38,299	$64,896	$85,636	-$20,740
2	14,289	10,734	1,476	35,185	61,683	81,122	-19,439
3	14,377	10,978	1,486	32,585	59,426	79,132	-19,706
4	14,466	11,229	1,495	35,065	62,255	82,232	-19,977
5	14,556	11,485	1,504	32,465	60,011	80,265	-20,254
6	14,646	11,747	1,513	35,065	62,972	83,509	-20,537
7	14,737	12,015	1,523	32,465	60,741	81,565	-20,824
8	14,829	12,290	1,532	35,065	63,715	84,833	-21,117

9	14,920	12,570	1,542	32,465	61,498	82,914	-21,416
10	15,013	12,858	1,551	35,065	64,487	86,207	-21,720
Total	$146,034	$116,401	$15,523	$343,725	$621,684	$827,415	-$205,731

Note: Totals may not add due to rounding.

Table 20 presents the total costs using the aforementioned adjusted values from the sensitivity analysis. As shown, the total costs to industry under the sensitivity analysis based on the altered assumptions for the main cost drivers are $2.1 billion. This cost includes the adjusted costs of the three industries included in the sensitivity (freight rail, PTPR, and pipeline) as well as the unadjusted, undiscounted cost to OTRB entities (see Table 9). The difference from the primary analysis presented in Table 10 is $1.0 billion (a 33 percent reduction).

TABLE 20: TOTAL COSTS UNDER THE SENSITIVITY ANALYSIS ($ THOUSANDS)

Year	Total regulated industries sensitivity analysis cost	TSA sensitivity analysis cost	Total proposed rule sensitivity analysis cost		
			Undiscounted	Discounted at 3%	Discounted at 7%
	a	b	c = ∑a,b		
1	$205,829	$4,426	$210,256	$204,132	$196,501
2	200,638	2,408	203,046	191,390	177,348
3	197,527	2,412	199,939	182,972	163,210
4	204,215	1,358	205,573	182,649	156,831
5	201,172	1,363	202,535	174,709	144,405
6	208,165	1,368	209,533	175,481	139,621
7	205,186	1,372	206,559	167,951	128,634
8	212,254	1,377	213,632	168,643	124,336
9	209,347	1,382	210,729	161,506	114,623
10	216,492	1,387	217,879	162,123	110,759
Total	$2,060,827	$18,854	$2,079,681	$1,771,556	$1,456,266
Annualized			$207,968	$207,680	$207,340

Note: Totals may not add due to rounding.

TSA requests public comment on the assumptions and estimates presented in the primary cost analysis as well as those within this sensitivity both of which may be used to better inform, update, or improve the overall analysis.

c. Benefits

The primary benefit of the proposed rule is a potential reduction in the risk of cybersecurity incidents as well as the impact of any such incident. The CRM program could enhance cybersecurity by reducing vulnerability to cybersecurity incidents by

having defense mechanisms in place that increase owner/operator ability to monitor and mitigate threats as well as strengthening response measures in the event of a cybersecurity incident. Specifically, the proposed rule would require designated owner/operators for three of the four modes to identify a Cybersecurity Coordinator and report cybersecurity incidents. Owner/operators of freight railroads, PTPR, and pipeline facilities and systems that meet the applicability criteria would also be required to develop and implement a comprehensive CRM program.

The proposed CRM program includes three primary elements. First, covered owner/operators would be required to regularly conduct an enterprise-wide cybersecurity evaluation that would identify their current cybersecurity profile. Benefits of regular cybersecurity evaluations, such as through the rule's CSE requirement, and monitoring over time, include focusing attention on cybersecurity issues and initiatives, providing a means to assess or evaluate cyber-related threats and mitigation measures' evolution, as well as prioritizing response to address vulnerabilities effectively and informing budgeting and investments decisions for upgrade cycles and long-term improvements.[232]

Second, owner/operators would be required to develop a COIP with requirements that focus on: (a) governance of the CRM program that helps ensure its successful implementation, relevance, and ability to address cybersecurity matters; (b) identification of critical cyber systems to help prioritize and optimize efforts; (c) protecting critical cyber systems that help minimize unnecessary network traffic, control internal network access points for users, shorten network downtime and increase reliable operational uptime, stop threats more quickly, as well as minimize the risks associated with lost data; (d) detecting and monitoring critical cyber systems to help detect incidents sooner and

---

[232] *See* NIST SP 800-53, Revision 5. Security and Privacy Controls for Information Systems and Organizations, available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf (last accessed July 25, 2024); *see also* NIST SP 800-37, Revision 2. Risk Management Framework for Information Systems and Organizations, available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf (last accessed July 25, 2024).

respond to incidents more quickly, potentially reducing the associated impacts; and (e) ensuring response and recovery to help ensure efficient and effective restoration of operational capabilities following an incident. As part of this COIP process to ensuring response and recovery, owner/operators would develop a CIRP that would require an established set of policies and procedures in place to respond to intrusions into their critical cybersecurity systems and maintenance or reconstitution of operations during an incident. Reduction in time and confusion with how they respond to future incidents provides a benefit to owner/operators, passengers/consumers, and society.

Third, owner/operators would be required to have a CAP that includes an independent evaluation of the effectiveness of their CRM program and identification of unaddressed vulnerabilities that helps establish greater accountability. Independent evaluation will ensure that the assessments, audits, testing, and other assessment capabilities would not be conducted by individuals who have oversight or responsibility for implementing the owner/operators CRM program and have no vested or other financial interest in the results.

The proposed rule would also expand the requirement for having a Physical Security Coordinator (currently in 49 CFR 1570.201) and reporting significant physical security concerns (currently in 49 CFR 1570.203) to owner/operators of designated pipeline facilities and systems, which helps delineate clear communication channels by establishing a single point of contact and creates greater awareness of the various types of cybersecurity threats encountered.

The proposed rule's CRM program requirements could create benefits through the identification, protection, detection, response, and recovery from cybersecurity threats which are discussed more fully in the RIA. Identifying a standardized requirement applicable to owner/operators that meet applicability criteria, would also provide more consistent application of and investments in cybersecurity measures yet offer flexibility

by focusing on security outcomes which allows for innovation and the unique operational aspects for each owner/operator. In addition, applicability criteria based on the volume of passengers or goods transported, as opposed to entity size, focuses requirements on owner/operators where there is the greatest potential impact, including small entities that play a critical role or function. Further, the proposed requirements would encourage greater investment and development of cybersecurity measures, potential pooling of resources to address common issues, as well gains in efficiencies over time which would reduce the direct and indirect costs of cybersecurity incidents.

d. Break-even Analysis

TSA uses a break-even analysis to help understand and frame the relationship between the potential benefits of the proposed rule and the costs of implementation.[233] Consistent with OMB Circular No. A–4, "Regulatory Analysis," this analysis answers the question "How small could the value of the non-qualified benefits be (or how large would the value of the non-quantified costs need to be) before the rule would yield zero net benefits?"[234]

A break-even analysis estimates a threshold value for the security benefits of the proposed rule so that the benefits of the rulemaking exactly match its costs. TSA compared potential consequence levels of cybersecurity incidents to the annualized cost (discounted at 7 percent) to industry and TSA from the proposed rule for each mode to estimate how often a cybersecurity incident of that size would need to be averted for the expected benefits to equal estimated costs for that transportation mode.

As part of calculating the break-even point of an analysis, TSA uses the full cost of the cybersecurity provisions of the proposed rule (physical security related

---

[233] When it is not possible to quantify or monetize a majority of the incremental benefits of a regulation, OMB recommends conducting a threshold, or "break-even" analysis.

[234] OMB, "Circular A–4: Regulatory Analysis," Section B. The Need for Federal Regulatory Action. Sept. 17, 2003. pg. 2.

requirements are not included) to assess the level of benefits or avoided costs required to break even.[235] Applying the simplest version of the conclusion, if the proposed rule prevents annual costs of approximately $307.8 million (at 7 percent) across all impacted surface modes, its benefits will justify its costs.

TSA also calculates the prevention of costs necessary for freight rail, PTPR, and pipeline independently using CRM program costs identified in Tables 21, 22, and 23. These tables also present a selection of break-even scenarios of varying magnitudes to illustrate the level of risk reduction necessary for such sized events to break-even. Specifically, they include the annualized cost of the cybersecurity focused provisions of the proposed rule (discounted at 7 percent) along with identified consequence levels or avoided losses. Those values are divided by each other to derive the required risk reduction and frequency of averted cybersecurity incidents to break even with respect to the cost of the CRM program of the proposed rule.

Table 21 presents the amount of risk reduction necessary for a range of consequence levels relative to freight rail estimated CRM program costs. TSA uses the AAR's estimate that a complete nationwide shutdown of freight rail transportation could cost the U.S. economy more than $2 billion a day as a basis for potential impact.[236] Based on this figure, even if only a fractional amount of the system were incapacitated or operated at reduced capacity it would result in substantial impacts depending on the number of days affected. The CRM rule would reduce the likelihood of the type of systemic disruption that would occur from a wide scale attack through the regulation of the largest and most interconnected owner/operators. If an attacker were to gain access to a freight rail entity's IT system and further penetrate the OT system, such an attacker

[235] TSA uses the full cost of the CRM program and cybersecurity related costs in this break-even analysis without adjusting for costs industry has incurred as a result of prior industry practices or TSA SDs.
[236] AAR, *The Economic Impact of a Railroad Shutdown* at 2 (2022), available at https://www.aar.org/wp-content/uploads/2022/09/AAR-Rail-Shutdown-Report-September-2022.pdf (last accessed Sept. 28, 2023).

could cause rail service interruptions for that entity and potential wider cascading effects, especially if multiple owner/operators were attacked simultaneously. The CRM rule would reduce the likelihood of such an attack occurring through the protections implemented in the COIP, such as network segmentation, access control and patch management. If the attack partially succeeded, the CRM rule would reduce the impact of such an incident due to the requirements to develop plans to detect, respond to and recover from cybersecurity incidents as part of the COIP. TSA shows break-even levels based on $1 billion, $10 billion, and $20 billion consequence levels by comparing the magnitude of the consequences to the annualized cost of the proposed CRM rule discounted at 7 percent.

TABLE 21: FREIGHT RAIL SUMMARY OF CRM PROGRAM BREAK-EVEN RESULTS

Break-even Example	Annualized cost of CRM program (7% discount rate)	Consequence (avoided losses)	Required risk reduction	Required frequency of averted cybersecurity incidents
	a	*b*	$c = a \div b$	$d = b \div a$
1 billion dollar example	$98.22 million	$1 billion	0.0982	One every 10.18 years
10 billion dollar example		10 billion	0.0098	One every 101.81 years
20 billion dollar example		20 billion	0.0049	One every 203.62 years

Table 22 presents the amount of risk reduction necessary for a range of consequence levels relative to PTPR estimated CRM program costs. The type of incident and size of the ridership impacted would greatly impact the level of consequence. For instance, shutting down municipal rail services for under a million passengers for a day is different than shutting down and/or delaying services of multiple million for a prolonged period of time. In such cases, the impact may largely represent delays in time and inconvenience while other instances, they may include train derailments or collisions that result in loss of life. If an attacker were to gain access to a transit entity's IT system and without sufficient network segmentation further penetrate the OT system, such an attacker could cause service interruptions for that entity's riders by impacting critical systems that prevent travel or disrupt safety measures that could require trains to operate at reduced speeds or potentially cause them to derail/collide. The CRM rule would

reduce the likelihood of such an attack occurring through the protections implemented in the COIP like network segmentation, access control and patch management.[237] If the attack partially succeeded, the CRM rule would reduce the impact of such an incident due to the requirements to develop plans to detect, respond to and recover from cybersecurity incidents as part of the COIP. TSA shows break-even levels based on $1 billion, $2 billion, or $4 billion consequence levels by comparing the magnitude of the consequences to the annualized cost of the proposed CRM rule discounted at 7 percent.

TABLE 22: PTPR SUMMARY OF CRM PROGRAM BREAK-EVEN RESULTS

Break-even example	Annualized cost of CRM program (7% discount rate)	Consequence (avoided losses)	Required risk reduction	Required frequency of averted cybersecurity incidents
	a	*b*	*c = a ÷ b*	*d = b ÷ a*
1 billion dollar example	$125.74 million	$1 billion	0.1257	One every 7.95 years
10 billion dollar example		2 billion	0.00629	One every 15.91 years
20 billion dollar example		4 billion	0.0314	One every 31.81 years

Table 23 presents the amount of risk reduction necessary for a range of consequence levels relative to pipeline estimated CRM program costs. The national pipeline system transports hazardous liquids, natural gas, and other liquids and gases that are used by various other segments of the economy including supplying materials for energy needs and manufacturing. Disrupting the transportation of these materials can have widespread effects that increase in magnitude depending on the pipelines impacted and the disruptions length of time. If an attacker were to gain access to a pipeline entity's IT system and without sufficient network segmentation further penetrate the OT system, such an attacker could cause product delivery interruptions for that entity or a wider set of pipeline network effects by causing damages to extensive portions of pipeline or critical/large junctions. Consistent with the above discussion on rail, the CRM rule would reduce the likelihood of such an attack occurring through the protections

[237] *See* Dragos Year in Review, 2022. There is discussion on the 39 percent fluctuation changes in oil/gas industries (Table 5: Poor Security Perimeters by OT Industry) which is likely correlated to the implementation of the TSA SDs released in response to the ransomware attack on a major pipeline company in 2021.

implemented in the COIP like network segmentation, access control and patch management.[238] If the attack partially succeeded, the CRM rule would reduce the impact of such an incident due to the requirements to develop plans to detect, respond to and recover from cybersecurity incidents as part of the COIP. Given the expansive impact pipeline products have on various aspects of the economy, TSA assumes a widespread disruption to the system could range from $1 to $2 billion per day. Based on this figure, even if only a fractional amount of the system were disrupted or operated at reduced capacity, this disruption could result in substantial impacts depending on the number of days affected. TSA shows break-even levels based on $2 billion, $10 billion, and $20 billion of consequence compared to the annualized cost of the proposed CRM rule discounted at 7 percent.

TABLE 23: PIPELINE SUMMARY OF FULL CRM PROGRAM BREAK-EVEN RESULTS

Break-even example	Annualized cost of CRM program (7% discount rate)	Consequence (avoided losses)	Required risk reduction	Required frequency of averted cybersecurity incidents
	a	*b*	*c = a ÷ b*	*d = b ÷ a*
2 billion dollar example	$83.667 million	$2 billion	0.0418	One every 23.90 years
10 billion dollar example		10 billion	0.0084	One every 119.52 years
20 billion dollar example		20 billion	0.0042	One every 239.04 years

TSA also compares the potential levels of consequence to the estimated costs of the CRM rule under its cost sensitivity assumptions discussed above. For Freight Rail the annualized cost of the rule discounted at 7 percent falls from $98.22 million in the primary proposal to $65.95 million in the sensitivity analysis. Freight Rail risk reduction is reduced by 33 percent in direct proportion to the 33 percent reduction in cost. Consequently, each of the contemplated $1 billion, $10 billion, and $20 billion consequence attacks need to be prevented less frequently for the proposed rule's costs and benefits to balance.

TABLE 24: FREIGHT RAIL SUMMARY OF SENSITIVITY CRM PROGRAM BREAK-EVEN RESULTS

Break-even example	Annualized cost of CRM program (7% discount rate)	Consequence (avoided losses)	Required risk reduction	Required frequency of averted cybersecurity incidents
	a	*b*	*c = a ÷ b*	*d = b ÷ a*
1 billion dollar example	$65.949 million	$1 billion	0.0659	One every 15.16 years
10 billion dollar example		10 billion	0.0066	One every 151.63 years
20 billion dollar example		20 billion	0.0033	One every 303.27 years

For the PTPR mode, the annualized cost of the proposed rule discounted at 7 percent falls from $125.74 million in the primary proposal to $78.06 million in the sensitivity analysis. PTPR risk reduction is reduced by 38 percent in direct proportion to

[238] *Id.*

the 38 percent reduction in cost. Consequently, each of the contemplated $1 billion, $2 billion, and $4 billion consequence attacks need to be prevented less frequently for the proposed rule's costs and benefits to balance.

TABLE 25: PTPR SUMMARY OF SENSITIVITY CRM PROGRAM BREAK-EVEN RESULTS

Break-even example	Annualized cost of CRM program (7% discount rate)	Consequence (avoided losses)	Required risk reduction	Required frequency of averted cybersecurity incidents
	a	*b*	*c = a ÷ b*	*d = b ÷ a*
1 billion dollar example	$78.063 million	$1 billion	0.0781	One every 12.81 years
10 billion dollar example		2 billion	0.0390	One every 25.62 years
20 billion dollar example		4 billion	0.0195	One every 51.24 years

And finally, for the pipeline mode, the annualized cost of the proposed rule discounted at 7 percent falls from $83.69 million in the primary proposal to $63.22 million in the sensitivity analysis. Pipeline risk reduction is reduced by 25 percent in direct proportion to the 25 percent reduction in cost. Consequently, each of the contemplated $2 billion, $10 billion, and $20 billion consequence attacks need to be prevented less frequently for the proposed rule's costs and benefits to balance.

TABLE 26: PIPELINE SUMMARY OF SENSITIVITY CRM PROGRAM BREAK-EVEN RESULTS

Break-even example	Annualized cost of CRM program (7% discount rate)	Consequence (avoided losses)	Required risk reduction	Required frequency of averted cybersecurity incidents
	a	*b*	*c = a ÷ b*	*d = b ÷ a*
2 billion dollar example	$63.222 million	$2 billion	0.0316	One every 31.63 years
10 billion dollar example		10 billion	0.0063	One every 158.17 years
20 billion dollar example		20 billion	0.0032	One every 316.35 years

As devastating as the direct impacts of a successful cybersecurity incident can be in terms of the immediate loss of life and property, avoiding the impacts of the more difficult to measure indirect effects are also substantial benefits of preventing a cybersecurity incident. For instance, should there be a cybersecurity incident impacting a public transit system, potential ripple impacts could include additional hardship on individuals who would then have to find alternate means of transportation. This use of alternate means of transportation would likely lead to increased traffic and commuting times on roadways, which has costs both in terms of additional gasoline and accrued wear and tear at the micro level but also compounded environmental effects at the macro level. A more detailed discussion of the break-even analysis and review of potential

consequence with some illustrative examples can be found in Section 4.2 of the RIA.

Although the break-even analysis considers each example separately, it is more likely that a combination of preventing all these scenarios and others would provide the benefits from these requirements. Cybersecurity incidents could carry considerable consequences in terms of equipment damages, disruption of services, and even loss of life. The impacts can reach billions of dollars depending on the scope of the incident; therefore, preventing even a small number of such potential incidents can justify the cost of the CRM program.[239]However, considering the potentially high costs of future cybersecurity incidents, including the (unquantifiable but real) risk of high-cost or potentially catastrophic incidents, TSA believes that the benefits of the proposed rule are likely to justify its costs.

3. OMB A–4 Statement

The OMB A–4 Accounting Statement presents annualized costs and qualitative benefits of the proposed rule.

TABLE 27: OMB A-4 ACCOUNTING STATEMENT

Category	Estimates			Units			Notes
	Primary	Low	High	Year Dollar	Discount Rate	Period Covered	
Benefits							
Annualized Monetized (millions/year)	N/A	N/A	N/A	N/A	7%	N/A	Not Quantified
	N/A	N/A	N/A	N/A	3%	N/A	
Annualized Quantified	N/A	N/A	N/A	N/A	7%	N/A	Not Quantified
	N/A	N/A	N/A	N/A	3%	N/A	
Qualitative	The requirements proposed in this rule, if finalized, could produce benefits by reducing cybersecurity risk and service interruptions of owner/operators in affected modes and help strengthen systems against cybersecurity incidents. Additionally, benefits would be produced by increasing the security of passengers, crew, and the general public.						
Costs							
Annualized Monetized (millions/year)	$307.76	N/A	N/A	2022	7%	10 Years	NPRM RIA
	$308.43	N/A	N/A	2022	3%	10 Years	
Annualized Quantified	N/A	N/A	N/A	N/A	7%	N/A	None
	N/A	N/A	N/A	N/A	3%	N/A	
Qualitative	Qualitative costs include those related to actual mitigation measures implemented and not otherwise covered as a result of the rule, as well as the cost incurred as a result of the COIP amendment process. Additional administrative costs may also be incurred during the						

[239] See break-even analysis section 4.3 in the RIA for details.

TABLE 27: OMB A-4 ACCOUNTING STATEMENT

Category	Estimates			Units			Notes
	Primary	Low	High	Year Dollar	Discount Rate	Period Covered	
	implementation process beyond what TSA has estimated.						
Transfers							
Federal Annualized Monetized (millions/year)	N/A	N/A	N/A	N/A	7%	NA	None
	N/A	N/A	N/A	N/A	3%	NA	
From/To	From:			To:			
Other Annualized Monetized (millions/year)	N/A	N/A	N/A	N/A	7%	NA	None
	N/A	N/A	N/A	N/A	3%	NA	
From/To	From:			To:			
Effects							
State, Local, and/or Tribal Government	State and Local governments are impacted by the requirements related to passenger rail and rail transit. These modes are primarily owned and operated by State and local governments.						None
Small Business	Prepared IRFA.			NA	NA	NA	NPRM IRFA
Wages	None.						
Growth	Not Measured.						

4. Alternatives considered

In addition to the proposed rule, TSA also considered three alternative regulatory options to the primary alternative reviewed in the analysis. The first alternative is to implement a limited scope of requirements. The second alternative is to reduce the applicability of the rule across the industries being regulated. The third alternative is to add regulatory requirements that mandate vetting, including a terrorism/other analyses check and immigration check for all frontline workers in the pipeline industry, as well as a terrorism/other analyses check, immigration check, and a CHRC for all Cybersecurity Coordinators and accountable executives in all industries.

Alternative 1 would limit the rule to the following requirements:

- Governance of the CRM program (proposed sections 1580.309, 1582.209, and 1586.209)
- Cybersecurity Coordinator (proposed sections 1580.311, 1582.211, and 1586.211)
- Identification of Critical Cybersecurity Systems (proposed sections 1580.313,

1582.213, and 1586.213)

- Reporting Cybersecurity Incidents (proposed sections 1580.325, 1582.225, and 1586.225)
- Cybersecurity Incident Response Plan (proposed sections 1580.327, 1582.227, and 1586.227).

These requirements identify responsible persons and organizations for an owner/operator's CRM program, identify the cybersecurity systems, require the reporting of cybersecurity incidents to CISA, and require the submission of a CIRP. This alternative includes some of the provisions in TSA's current SDs but does not require owner/operators to implement measures necessary to meet all the proposed security outcomes to protect against ransomware attacks and other known threats to IT and OT systems, nor to conduct a cybersecurity evaluation or have a robust assessment program. Any other security requirements or program implementation would be up to the owner/operator to establish and implement voluntarily for themselves. This alternative would still enable TSA to maintain oversight at a reactionary level, but it would reduce visibility into implementation of any preventative efforts.

Alternative 2 would shrink the applicability of the requirements to the largest owner/operators in each of the regulated industries. This alternative would reduce the freight rail applicability to cover a population limited to only Class I rail lines as defined by the Surface Transportation Board, resulting in a scope of just six owner/operators. The PTPR applicability would cover a population limited to just owner/operators who host Class I freight railroads/Amtrak lines or those who have an average daily ridership of 100,000 passengers in any of the previous 3 years or at any time in the future. This covers a current population of 27 owner/operators, down from 34 in the preferred alternative, and would reduce the ridership protected to around 90 percent of daily ridership nationwide. For the regulated pipeline owner/operators, this alternative would

change the applicability to the 98 critical owner/operators of hazardous liquid and natural gas pipelines and liquefied natural gas facilities.

Alternative 3 would introduce a requirement for accountable executives and Cybersecurity Coordinators, in all covered entities, to receive a Level 3 STA.[240] Furthermore, this alternative would require all frontline workers ("security-sensitive employees") in the pipeline industry to undergo a Level-2 STA, consistent with the proposed requirements for security-sensitive requirements in the Security Vetting of Certain Transportation Workers Rulemaking.[241]

Table 28 shows a comparison of the cost of the alternatives considered.

TABLE 28: COMPARISON OF COSTS BETWEEN PROPOSED RULE AND ALTERNATIVES (DISCOUNTED AT 7%, THOUSANDS)

Regulatory action	Initial affected population (number of owner/ operators)	Ten-year costs			Annualized costs		
		Industry	TSA	Total	Industry	TSA	Total
		a	b	c = ∑a,b	d	e	f = ∑d,e
Proposed Rule	Freight Rail – 73 PTPR – 34 OTRB – 71 Pipeline - 115	$2,147,313	$14,241	$2,161,554	$305,729	$2,028	$307,757
Alternative 1	Freight Rail – 73 PTPR – 34 OTRB – 71 Pipeline - 115	81,555	2,377	83,932	11,612	338	11,950
Alternative 2	Freight Rail – 6 PTPR – 27 OTRB – 0 Pipeline - 98	1,419,861	10,264	1,430,125	202,156	1,461	203,618
Alternative 3	Freight Rail – 73 PTPR – 34 OTRB – 71 Pipeline - 115	2,160,147	14,241	2,174,389	307,556	2,028	309,584

Although not the least costly option, TSA presents the proposed rule as its preferred option. Alternative 1 has a smaller up-front cost but is less proactive. Based on the recentness of the SDs, the extent that some companies are already implementing adequate cybersecurity policies consistent with the guidelines described in this rulemaking, and internal TSA data from 2021/2022, the industry was failing to

[240] Under the proposed rule, accountable executives and Cybersecurity Coordinators for all covered entities, would not receive an STA.
[241] *See* https://www.regulations.gov/docket/TSA-2023-0001 (last accessed July 5, 2023).

implement preventative measures on its own. As a result, limiting the scope of the requirements, as Alternative 1 does, produces an unacceptable level of risk for TSA. Reducing the scope would remove the requirement from some entities to meet specific cybersecurity performance measures to protect against cybersecurity incidents that could threaten the availability, integrity, and confidentiality of data on and traversing IT and OT systems, to conduct a cybersecurity evaluation, and have an assessment plan. These proactive cybersecurity actions, evaluations, and assessments are considered best practices. Reducing the scope of the CRM in this fashion would increase the vulnerability of the covered operators to a host of cybersecurity incidents and impacts the CRM is designed to address.

Alternative 2 also has a smaller cost. This alternative, however, might increase the risk to the surface transportation infrastructure as it does not cover many entities TSA considers important. This increased risk reduction is important based on the role these entities and industries play in the supply chain, movement of people and goods, and their respective regional economies. Short line and regional railroads provide interconnectedness among the nation's rail customers and are a critical facet of the overall railroad industry. Leaving these railroads out of the applicability pool may result in critical terminal and switching services in addition to the pickup and delivery portions of the railroad being more vulnerable and susceptible to cybersecurity incidents. Due to the interconnectedness of the nation's rail system, if the connecting railroads are immobilized, cross-county rail service provided by the Class 1 railroads and its ability to move cargo may also be impacted thus having larger cascading effects.

For PTPR, the criteria of the preferred alternative apply to the high consequence operators and cover most of the national daily rail ridership. Reducing the scope of the covered entities in Alternative 2 reduces the level of the commuting population protected by the proposed cybersecurity performance measures and thus they are still exposed to a

higher level of risk. If a cybersecurity incident affected one of these entities, the damages and consequences could have a cascading effect beyond just the target and into the local and regional communities.

A reduction in covered pipeline operators could affect risk mitigation of potential operational disruption which could have widespread impacts. For instance, a cybersecurity incident affecting a control room that operates multiple pipeline systems, or impacting multiple pipelines, could lead to a large cascading impact on pipeline delivery, which could disrupt the accessibility of needed product to the communities reliant on the pipeline product.

Alternative 3 is costlier than the proposed rule due to the additional requirements added. However, the primary benefit of this alternative is the potential to reduce insider threats from employees who may wish to do harm, which could be aggravated to the extent the employee has access to sensitive information and/or operations. Accountable executives and Cybersecurity Coordinators for all modes, and the frontline employees and Physical Security Coordinators for the pipeline industry, are not currently required to undergo a terrorism/other analyses check, immigration check, or a CHRC. Requiring these individuals to undergo a terrorism/other analyses check against government databases may enable TSA to identify individuals who may pose a security threat.

Although Alternative 3 is not included in the primary analysis at this time, TSA seeks comments from affected stakeholders on how the vetting of Cybersecurity Coordinators, accountable executives, and/or pipeline employees would impact their operations and costs. TSA specifically seeks data regarding how many of the entity's employees the entity has that would be subject to the vetting requirements. Based on comments received, TSA may consider including appropriate vetting requirements in a final rule. TSA notes that it has already proposed the vetting of frontline workers for freight rail and PTPR, and of security coordinators for freight rail, PTPR, and OTRBs in

a separate rulemaking.

5. Regulatory Flexibility Assessment

The RFA requires agencies to consider the impacts of their rules on small entities. TSA performed an IRFA to analyze the impact to small entities affected by the proposed rule. The following provides a summary of the full RIA, which is available in the docket for this rulemaking.

Under the RFA, the term "small entities" comprises small businesses, not-for-profit organizations that are independently owned, operated, and not dominant in their fields,[242] as well as small governmental jurisdictions with populations of less than 50,000.[243] TSA performed an IRFA of the impacts on small entities from this proposed rule in the first year of the analysis and found that it may affect an estimated 293 U.S. entities (73 corporate-level Class I, II, and III freight railroad owner/operators, 34 PTPR owner/operators, 71 OTRB owner/operators, and 115 pipeline owner/operators). TSA analyzed all the entities that would be affected by the proposed rule and TSA found that 35 percent of them would be considered small. The proposed rule would require small freight rail, PTPR, and pipeline entities to (a) designate a Cybersecurity Coordinator, (b) report cybersecurity incidents to CISA, (c) establish a CRM program, (d) familiarization, (e) compliance, and (f) recordkeeping. Additionally, pipeline owner/operators would have to designate a Physical Security Coordinator and report significant physical security concerns to TSA. OTRB entities would only have to report cybersecurity incidents to CISA.

Regulated entities have different requirements under the proposed rule, depending on their industry. Freight rail, PTPR, and pipeline owner/operators would be required to

---

[242] The definition of a small business varies from industry to industry to properly reflect the relative differences in size between industries. An agency must either use the U.S. Small Business Administration (SBA) definition for a small business or establish an alternative definition for the industry. TSA has adopted the SBA small business size standards for each relevant industry.

[243] Individuals and States are not considered "small entities" based on the definitions in the RFA (5 U.S.C. 601).

designate a Cybersecurity Coordinator, report cybersecurity incidents, and have a CRM program approved by TSA and incur costs associated with familiarization, compliance, and recordkeeping requirements. Pipeline owner/operators have additional requirements to designate a Physical Security Coordinator and report significant physical security concerns to TSA. TSA is proposing that OTRB owner/operators must report cybersecurity incidents to CISA, as well as incur familiarization costs. TSA estimates the proposed rule's requirements to cost $486,792 per entity for freight rail owner/operators, $682 per entity for OTRB owner/operators, and $484,848 per entity for pipeline owner/operators in the highest cost year of the proposed rule. TSA did not calculate the cost per entity for PTPR entities in this IRFA as none of the PTPR owner/operators are considered small. Separately, TSA estimates the proposed rule requirements to cost $537 per employee for freight rail entities, and $659 per employee for pipeline owner/operators. The proposed rule has zero cost per employee for OTRB owner/operators, as the proposed requirements covering these entities (cybersecurity incident reporting) are not based on the number of employees and thus do not incur any associated per employee cost. TSA invites all interested parties to submit data and information regarding the potential economic impact on small entities that would result from the adoption of the requirements in the proposed rule.

TSA estimated the overall impact on small entities due to the proposed rule by adding the number of small entities affected (with revenue data available) in each revenue impact range for each of the four subgroups: freight rail, PTPR, OTRB and pipeline industries. Across the combined 293 covered entities, TSA estimates that 79 (27 percent) are considered small. Of these small entities, TSA found employment and revenue data on 75 entities. The IRFA finds that 11 of the analyzed entities would have an impact greater than one percent of their annual revenue. Table 29 presents the likely distribution of impact for small owner/operators.

TABLE 29: AVERAGE COST IMPACT ON SMALL ENTITIES AS A PERCENTAGE OF REVENUE

Revenue Impact Range	Freight Rail (# of Affected Small Entities)	Freight Rail (% of Affected Small Entities)	OTRB (# of Affected Small Entities)	OTRB (% of Affected Small Entities)	Pipeline (# of Affected Small Entities)	Pipeline (% of Affected Small Entities)	Total (# of Affected Small Entities)	Total (% of Affected Small Entities)
0% < Impact ≤ 1%	6	35	55	100	7	100	68	86.1
1% < Impact ≤ 3%	3	18					3	3.8
3% < Impact ≤ 5%	4	24					4	5.1
5% < Impact ≤ 10%	2	12					2	2.5
Above 10%	2	12					2	2.5
Total	17	100	55	100	7	100	79	100

An identification, to the extent practicable, of all relevant federal rules which may duplicate, overlap, or conflict with the proposed rule.

As noted by the ONCD in an August 2023 Request for Information, the National Cybersecurity Strategy calls for establishing cybersecurity regulations to secure critical infrastructure where existing measures are insufficient; harmonizing and streamlining new and existing regulations; and enabling regulated entities to afford to achieve security.[244] TSA emphasizes its commitment to regulatory harmonization and streamlining, and notes that this proposed rule, which is grounded in NIST's Framework for Improving Critical Infrastructure Cybersecurity, NIST's standards and best practices, and the CISA CPGs, is consistent with such priorities. TSA also acknowledges the ongoing rulemakings of other DHS components, including ongoing rulemakings on cybersecurity in maritime transportation and implementation of CIRCIA. TSA notes potential differences in terminology and policy as compared to those rulemakings; although TSA views such differences as intentional and based on sector-specific distinctions, TSA welcomes comments on opportunities to harmonize and streamline regulations where feasible and appropriate.

[244] *See* Request for Information on Cyber Regulatory Harmonization; Request for Information: Opportunities for and Obstacles to Harmonizing Cybersecurity Regulations, 88 FR 55694 (Aug. 16, 2023).

For pipeline owner/operators, TSA will coordinate activities under this part with the FERC, and the PHMSA of the DOT with respect to regulation of pipeline systems and facilities that are also licensed or regulated by the FERC or PHMSA, to avoid conflicting requirements and minimize redundancy of compliance activities.

TSA is also aware that some pipeline owner/operators may also have other business lines in the energy sector that are subject to regulations issued by DOE, and FERC's cybersecurity standards as issued by the NERC. TSA has committed to reducing the impact on these multi-sector companies by aligning the agency's proposed requirements with the NIST CSF, which is also used by the DOE, FERC, and NERC.[245]

TSA is currently participating in a forum of regulatory agencies looking at opportunities for harmonization and reciprocity for cybersecurity requirements. In addition, CISA is required by CIRCIA[246] to issue a rule to implement a 72-hour covered cyber incident reporting requirement and 24-hour ransom payment reporting requirement for ransom payments made in connection with a ransomware attack. These requirements would be applicable to covered entities across critical infrastructure sectors, as further defined by CISA through rulemaking. Although this NPRM and CISA's rulemaking could technically create two cyber incident reporting requirements for some entities, TSA does not believe that this is likely to result in any actual duplicative reporting because entities subject to the cybersecurity incident reporting requirements proposed in this NPRM would be required to make their reports to CISA. Currently, TSA has determined CIRCIA does not require TSA to modify its proposed reporting requirements. TSA will, however, re-assess its proposed requirements as CISA's rule is finalized to avoid any unnecessary conflicts or redundancies. TSA is committed to working with CISA to

---

[245] *See* NERC CIP-003-8, *Critical Infrastructure Protection Reliability Standards, Cyber Security – Security Management Controls,* and CIP-008-6 *(Cyber Security – Incident Reporting and Response Planning)*, available at https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-003-8.pdf and https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-008-6.pdfva (last accessed July 5, 2023).
[246] Division Y of Public Law No. 117-103, 136 Stat. 49 (Mar. 15, 2022).

ensure that entities required to report to CISA under both CIRCIA and this proposed rule, if any, can do so in a single report where legally possible. If necessary to do so, CISA and TSA will explore leveraging an exemption in CIRCIA for covered entities that are required to report substantially similar information to another Federal agency within a substantially similar timeframe, where CISA and the Federal agency have an agreement and information sharing mechanism in place. Currently, TSA has determined CIRCIA does not require TSA to modify its proposed reporting requirements. TSA will, however, re-assess its proposed requirements as CISA's rule is finalized to avoid any unnecessary conflicts or redundancies.

A Description of Any Significant Alternatives to the Proposed Rule That Accomplish the Stated Objectives of Applicable Statues and May Minimize Any Significant Economic Impact of the Proposed Rule on Small Entities, Including Alternatives Considered

The first regulatory alternative TSA considered would limit the scope of requirements. This alternative would include provisions requiring the owner/operator to identify responsible persons and organizations for an owner/operator's CRM program, identify the owner/operator's cybersecurity systems, the reporting of cybersecurity incidents to CISA/TSA, and the submission of an incident response plan. Any other security requirements or program implementation would be up to the owner/operator to establish and implement voluntarily for themselves. This alternative would still enable TSA to maintain oversight in a more reactive posture, but it would eliminate visibility of any preventative efforts owner/operators are undertaking and would not ensure the necessary baseline of cybersecurity measures is being consistently implemented across these higher-risk operations.

Unlike the proposed rule, Alternative 1 would have no per employee costs, as well as reduce the number of per entity costs. TSA did not evaluate the impact to small

entities for PTPR and OTRB owner/operators under this alternative as none of the PTPR owner/operators identified by TSA are considered small under the SBA size standards and OTRB owner/operators would be excluded under the applicability of this alternative.

TABLE 30: TOTAL COST PER OWNER OPERATOR ALTERNATIVE 1

Requirement	Unit time (hours)	Hourly wage rate	Unit cost
	a	b	c = b x a
Freight Rail			
Familiarization	15	$129.88	$1,904
Cybersecurity Incident Reporting	0.14	$97.22	$14
CRM program	87	$95.39	$8,299
CIRP	300	$94.36	$28,308
		Cost per Entity	$38,524
			Pipeline
Familiarization	56	$126.67	$7,093
Cybersecurity Incident Reporting	3	$94.55	$329
CRM program	87	$119.38	$10,386
CIRP	300	$89.84	$26,953
Cost per entity			$44,761

This alternative has lower estimated costs than the preferred alternative. TSA did not select it because it provides a reduced level of cybersecurity risk mitigation. TSA believes such mitigation is necessary given the key role these industries play in the supply chain, movement of people and goods, and the economy. This alternative would not require the visibility or accountability aspects of NIST's "detect" or "protect" elements that, when implemented as part of a cyber-risk management program, would help prevent malicious actors from exploiting vulnerabilities as well as ensure the confidentiality, availability, and integrity of their critical systems. Not including protecting critical cyber systems and having capabilities to respond to a cybersecurity incident reduces the level of protection when compared to the preferred alternative. Furthermore, a cybersecurity incident on any entity covered by the proposed rule, regardless of size, could have cascading impacts on the nation's economy.

Dynamic and emerging cybersecurity threats to the nation's rail and hazardous liquid and natural gas pipeline infrastructure require a more proactive approach toward reducing risk related to cybersecurity. In this case, TSA believes risk-based cybersecurity policy is the most effective means to mitigate the effects of potential cybersecurity incidents on critical infrastructure while minimizing costs to both industry and government. Exempting an entity solely based on its SBA-determined size would diminish the risk reduction this rulemaking is designed to achieve by failing to consider other criteria that may signal the critical value of the owner/operator to the transportation system.

The second alternative that TSA considered would limit the applicability of the requirements to the largest and most critical owner/operators in each of the regulated industries. This alternative would limit applicability of requirements for freight railroads to Class I Railroads, as defined by the Surface Transportation Board. For PTPR, requirements would be limited to owner/operators that host Class I Freight Rail Lines or those with an average daily ridership of 100,000 passengers in at least one of the last 3 years or in any future year. For pipelines, only the 98 most critical owner/operators of hazardous liquid and natural gas pipelines and liquefied natural gas facilities would be subject to the requirements. Under this more limited applicability, Alternative 2 would cover six Class I freight rail owner/operators, 27 PTPR agencies, and 100 pipeline

owner/operators in the tenth year of the proposed rule. OTRB owner/operators would be excluded under this alternative.

While Alternative 2 has the same cost per entity as the preferred alternative, this alternative reduces the overall number of entities determined to be small. All freight rail owner/operators determined to be small under the proposed rule would be removed from applicability of the proposed rule under Alternative 2, as none of the Class 1 freight railroads are considered small. OTRB owner/operators would have the same requirements as the proposed rule; however, none of the small OTRB owner/operators have a cost impact greater than one percent of annual revenue under either the proposed rule or this alternative. The number of small pipeline owner/operators would decrease from 23 to 13.

From an RFA perspective, this alternative impacts fewer small entities than the proposed rule. However, TSA has determined this alternative produces an unacceptable level of risk given the key role these industries play in the supply chain, movement of people and goods, and the economy. There are owner/operators not covered under these criteria that play a critical role in contributing to the stability and security of the movement of people and goods. An incident to these owner/operators may still result in a ripple effect throughout the economy. TSA believes railroads that transport the largest volume of cargo, and freight railroads that serve as critical connections between Class I railroads or serve as vital links in the STRACNET, are critical to the transportation industry. A cybersecurity incident affecting any of these railroads, regardless of the size of the entity, would have the most significant impact on rail transportation, national security, and economic security. Similarly, pipeline systems and facilities that transport the largest volume of commodities, regardless of entity size, would lead to the potential for a sustained disruption in service should a successful cybersecurity incident affect their ability to support national security needs, including economic security. While TSA

acknowledges that Alternative 2 would have reduced impacts on small entities, due to the quantitative (volume) and qualitative (strategic) applicability criteria in the proposed rule, TSA does not believe making applicability exceptions based on SBA size standards is justified.

In addition, TSA performed a sensitivity analysis of three major cost drivers (access control costs, cybersecurity systems data backup costs, and cybersecurity training) to help understand and evaluate the practical impacts of the proposed rule versus the zero-baseline assumption used in the primary analysis. The sensitivity analysis assumes 25 percent of freight rail and pipeline entities are already in full compliance with identified requirements, and 25 percent are in partial compliance. While the assumptions in the IRFA sensitivity analysis would not result in an increased economic impact on small PTPR entities (because no PTPR entities covered by the NPRM are small entities) or affect the cost estimates for OTRB entities (because OTRB doesn't incur any of the costs modified in the sensitivity analysis and none have a cost impact greater than one percent of annual revenue), they would reduce cost impacts on small freight rail and pipeline entities and decrease the number that would incur a cost greater than one percent of annual revenues.[247]

6. International trade impact assessment

The Trade Agreement Act of 1979 prohibits Federal agencies from establishing any standards or engaging in related activities that create unnecessary obstacles to the foreign commerce of the United States. The Trade Agreement Act does not consider legitimate domestic objectives, such as essential security, as unnecessary obstacles. The statute also requires that international standards be considered and, where appropriate, that they be the basis for U.S. standards. TSA has assessed the potential effect of this

[247] The primary IRFA analysis estimates 18 freight rail and 10 pipeline entities will have costs greater than one percent of annual revenue. In the IRFA sensitivity analysis, 13 freight rail and 8 pipeline entities will have costs greater than one percent of annual revenue.

proposed rule and has determined this rulemaking would not have an adverse impact on international trade.

7. Unfunded mandates assessment

Title II of UMRA[248] establishes requirements for Federal agencies to assess the effects of their regulatory actions on State, Local, and Tribal governments as well as the private sector. Under section 202, UMRA requires Federal agencies to prepare a written statement, including a cost–benefit analysis, for proposed and final rules with "Federal mandates" that may result in expenditures by State, Local, and Tribal governments in the aggregate or by the private sector of $100 million (adjusted for inflation) or more in any year. Before an agency promulgates a rule for which a written statement is required, section 205[249] of UMRA generally requires identification and consideration of a reasonable number of regulatory alternatives, and adopting the least costly, most cost-effective, or least burdensome alternative that achieves the objectives of the rule. The provisions of section 205 do not apply when they are inconsistent with applicable law. Moreover, section 205 allows an agency to adopt an alternative other than the least costly, most cost-effective, or least burdensome alternative if the final rule includes an explanation about why that alternative was not adopted.

Before establishing any regulatory requirements that may significantly or uniquely affect small governments, including tribal governments, Federal agencies must develop under section 203[250] of UMRA a small government agency plan. The plan must provide for notifying potentially affected small governments; enabling officials of affected small governments to have meaningful and timely input in the development of regulatory proposals with significant federal intergovernmental mandates; and informing, educating, and advising small governments on compliance with the regulatory

---

[248] *See supra* note 222, as codified at 2 U.S.C. 1532.
[249] *Id.,* as codified at 2 U.S.C. 1535.
[250] *Id.,* as codified at 2 U.S.C. 1533.

requirements.

Section 4 of UMRA[251] includes several types of actions that are excluded from its requirements. Among these exclusions are regulations necessary for the national security. This rule is not subject to UMRA review because it is a regulation necessary for the national security of the United States. As noted in the National Cybersecurity Strategy, this rule is being promulgated because of national security concerns related to the protection of Critical Cyber Systems, the loss or disruption of which could have impacts on national security, including economic security.

B. Paperwork Reduction Act

The Paperwork Reduction Act of 1995 (PRA)[252] requires that DHS consider the impact of paperwork and other information collection burdens imposed on the public. Under the provisions of PRA section 3507(d), DHS must obtain approval from the OMB for each collection of information it conducts, sponsors, or requires through regulations.

This proposed rule would call for a collection of information under the PRA. Accordingly, DHS has submitted to OMB the proposed rule and this analysis, including the sections relating to collections of information.[253] As defined in 5 CFR 1320.3(c), "collection of information" includes reporting, recordkeeping, monitoring, posting, labeling, and other similar actions. This section provides the description of the information collection and of those who must collect the information as well as an estimate of the total annual time burden.

We ask for public comment on the proposed collection of information to help us determine, among other things—

- How useful the information is;
- Whether the information can help us perform our functions better;

---

[251] *Id.*, as codified at 2 U.S.C. 1503.
[252] 44 U.S.C. 3501 et seq.
[253] *See* 5 CFR 1320.11(a).

- How we can improve the quality, usefulness, and clarity of the information;
- Whether the information is readily available elsewhere;
- How accurate our estimate is of the burden of collection;
- How valid our methods are for determining the burden of collection; and
- How we can minimize the burden of collection.

Please see instructions under "Public Participation" for submission of comments on the information collection.

As protection provided by the PRA, as amended, an agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid OMB control number. OMB has previously approved an information collection request (ICR) for Pipeline Critical Infrastructure List under OMB Control Number 1652-0050, Pipeline Security Incident Reporting under OMB Control No. 1652-0055, Pipeline Corporate Security Reviews under OMB Control No. 1652-0056, and Cybersecurity Measures for Surface Modes under OMB Control No. 1652-0074. This proposed collection consolidates and replaces all current ICR requirements for CRM of freight rail, passenger rail, and pipeline owner/operators under one OMB control number. Upon approval of the new ICR and publication of a final rule, TSA will amend, or as appropriate rescind, the current ICRs associated with TSA SDs currently in effect. Even though most of the ICRs in the CRM NPRM are currently covered by approved ICRs, TSA is adding a few new requirements requiring information collection that were not previously included in TSA SDs or otherwise in approved ICRs.

These new requirements for all rail (freight, passenger, and transit) and pipeline owner/operators subject to the ICR include: (1) submission of a Cybersecurity training program to TSA for approval (reporting); (2) maintaining records of employee cybersecurity training (record keeping); and (3) maintaining records of inclusion of supply chain security measures in the owner/operator's COIP. OTRB owner/operators

are currently required to report significant security concerns and would also be required to report cybersecurity incidents.

Finally, the CRM NPRM proposes to add a new requirement for pipeline owner/operators to: (1) designate a physical security coordinator and submit the contact information to TSA and (2) report significant physical security concerns to TSA. This additional requirement for pipelines would align with requirements applicable to the other owner/operators covered by the proposed rule. Upon finalization of the CRM rulemaking, TSA will use the information collection to establish compliance with the new regulatory requirements. By implementing these performance-based requirements, TSA would ensure that the 293 higher-risk entities have measures in place to address current cybersecurity risks with the flexibility necessary to address emerging threats and deploy evolving capabilities, and that CISA and TSA are receiving information on cybersecurity threats from all higher-risk surface owner/operators identified by TSA, including 71 OTRB entities not currently subject to the SDs. Accordingly, TSA has submitted all information requirements to OMB for its review.

Table 31 shows the information collection and corresponding burden-hours for entities falling under the requirements of the proposed rule. The collections that have been implemented under the SD-related ICRs would continue or be updated under the proposed rule.[254]

TABLE 31: PRA BURDEN HOURS

Collection	Time Per Response (hours)	Number of Responses			3-Year Time Burden	Average Annual Time Burden
		Year 1	Year 2	Year 3		
Cybersecurity Evaluation (CSE)						
Freight Rail	40	73	74	74	8,829	2,943

[254] Rail security and rail cybersecurity information collection requirements resulting from the SDs covered under ICR 1652-0051 and 1652-0074. Pipeline security and cybersecurity information collection requirements from the SDs are covered under ICR 1652-0050, 1652-0055, and 1652-0056. For additional information, Table 1-2 in the RIA details the number of covered entities in the SD ICs and include the Published Notice title as well as the effective date.

TABLE 31: PRA BURDEN HOURS

Collection	Time Per Response (hours)	Number of Responses			3-Year Time Burden	Average Annual Time Burden
		Year 1	Year 2	Year 3		
PTPR	40	34	35	36	4,170	1,390
Pipelines	120	115	115	115	41,400	13,800
Submit COIP						
Freight Rail	40	73	73	74	8,783	2,928
PTPR	40	34	34	35	4,110	1,370
Pipelines	40	115	115	115	13,800	4,600
Submit POAM						
Freight Rail	80	15	15	15	3,531	1,177
PTPR	80	7	7	7	1,668	556
Pipelines	80	23	23	23	5,520	1,840
Accountable Executive Information Submission						
Freight Rail	3	73	4	4	240	80
PTPR	3	34	5	5	134	45
Pipelines	3	115	16	16	439	146
Cybersecurity Coordinator Information Submission						
Freight Rail	2	146	7	7	320	107
PTPR	2	68	10	11	178	59
Pipelines	2	230	9	9	497	166
Supply Chain Management						
Freight Rail	10	73	74	74	2207	736
PTPR	10	34	35	36	1,043	348
Pipelines	10	115	115	115	3450	1150
Physical Security Coordinator Information Submission						
Pipelines	0.50	261	36	36	166	55
Report Significant Physical Security Concerns to TSA						
Pipelines	0.05	2,908	2,908	2,908	436	145
Initial Cybersecurity Training Plan Development and Submission						
Freight Rail	80	73	1	1	5,931	1,977
PTPR	80	34	1	1	2,841	947
Pipelines	80	115	-	-	9,200	3,067
Cybersecurity Training Documentation Recordkeeping						
Freight Rail	0.02	134,504	135,064	135,626	6,753	2,251
PTPR	0.02	344,632	348,472	352,356	17,424	5,808
Pipelines	0.02	45,908	46,194	46,482	2,310	770
Report Cybersecurity Incidents to CISA						
Freight Rail	1	10	10	10	30	10
PTPR	1	15	15	16	15	15
OTRB	1	15	15	16	46	15
Pipelines	1	400	400	400	1,200	400

TABLE 31: PRA BURDEN HOURS

Collection	Time Per Response (hours)	Number of Responses			3-Year Time Burden	Average Annual Time Burden
		Year 1	Year 2	Year 3		
Cybersecurity Incident Response Plan (CIRP)						
Freight Rail	80	73	-	-	5,840	1,947
PTPR	80	34	-	-	2,720	907
Pipelines	80	115	-	-	9,200	3,067
CIRP Annual Exercise Recordkeeping						
Freight Rail	120	73	74	74	26,485	8,828
PTPR	120	34	35	36	12,510	4,170
Pipelines	120	115	115	115	41,400	13,800
Cybersecurity Assessment Plan (CAP)						
Freight Rail	44	73	74	74	9,711	3,237
PTPR	44	34	35	36	4,587	1,529
Pipelines	44	115	115	115	15,180	5,060
CAP Annual Report of Scheduled Testing (30 percent of CAP tested annually)						
Freight Rail	30	73	74	74	6,621	2,207
PTPR	30	34	35	36	3,128	1,043
Pipelines	30	115	115	115	10,350	3,450
Recordkeeping						
Freight Rail	2	73	74	74	441	147
PTPR	2	34	35	36	209	70
Pipelines	2	115	115	115	690	230
Total Number of Responses					1,606,559	535,520
Total Time Burden (hours)					363,858	121,286

C. Federalism (E.O. 13132)

A rule has implications for federalism under E.O. 13132 of August 4, 1999 (Federalism)[255] if it has substantial direct effects on the States, on the relationship between the national government and the States, or on the distribution of power and responsibilities among the various levels of government. TSA has analyzed this proposed rule under Executive Order 13132 and determined that it does not have implications for federalism. TSA welcomes public comments on Executive Order 13132 federalism implications.

[255] Published at 64 FR 43255 (Aug. 10, 1999).

D. Energy impact analysis (E.O. 13211)

DHS analyzed this proposed rule under E.O. 13211 of May 18, 2001 (Actions Concerning Regulations That Significantly Affected Energy Supply, Distribution or Use),[256] and determined that it is not a "significant energy action" under that E.O. and is not likely to have a significant adverse effect on the supply, distribution, or use of energy. Therefore, this rulemaking does not require a Statement of Energy Effects.

E. Environmental analysis

DHS reviews proposed actions to determine whether the National Environmental Policy Act (NEPA) applies to them and, if so, what degree of analysis is required. DHS Management Directive 023–01 Rev. 01 and Instruction Manual 023–01–001–01 Rev. 01 establish the procedures that DHS and its components use to comply with NEPA and the Council on Environmental Quality (CEQ)'s regulations for implementing NEPA.[257] The CEQ regulations allow Federal agencies to establish, with CEQ review and concurrence, categories of actions ("categorical exclusions") which experience has shown do not individually or cumulatively have a significant effect on the human environment and, therefore, do not require preparation of an Environmental Assessment or Environmental Impact Statement.[258]

The DHS categorical exclusions are listed in Appendix A of the Instruction Manual. Under DHS NEPA implementing procedures, for an action to be categorically excluded, it must satisfy each of the following three conditions: (1) The entire action clearly fits within one or more of the categorical exclusions; (2) the action is not a piece of a larger action; and (3) no extraordinary circumstances exist that create the potential for a significant environmental effect.

As previously discussed, this proposed rule would promote TSA's surface

---

[256] Published at 66 FR 28355 (May 22, 2001).
[257] *See* 40 CFR parts 1500 through 1508.
[258] *See* 40 CFR 1501.4, 1507.3(e)(2)(ii).

transportation security mission by establishing performance-based requirements to ensure higher-risk owner/operators have measures in place to address cybersecurity risks with the flexibility necessary to address emerging threats and deploy evolving capabilities. Specifically, this proposed rule would establish minimum cybersecurity requirements in TSA regulations such as account security measures, device security measures, governance and training, risk management, supply chain management, resilience, network segmentation, reporting, and physical security.

TSA has determined that this proposed rule clearly fits within categorical exclusion A3 in Appendix A of the Instruction Manual. Categorical exclusion A3 applies to promulgation of rules, issuance of rulings or interpretations, and the development and publication of policies, orders, directives, notices, procedures, manuals, advisory circulars, and other guidance documents of the following nature: (a) Those of a strictly administrative or procedural nature; (b) those that implement, without substantive change, statutory or regulatory requirements; (c) those that implement, without substantive change, procedures, manuals, and other guidance documents; (d) those that interpret or amend an existing regulation without changing its environmental effect; (e) technical guidance on safety and security matters; or (f) guidance for the preparation of security plans.

The requirements proposed in this rule are administrative in nature, providing technical guidance and instruction on safety and security matters and the preparation of security plans. TSA has further determined that the changes proposed in this rule would not result in any significant impact on the environment and, therefore, would not result in any "change in environmental effect." TSA further finds no extraordinary circumstances associated with this proposed rule that may give rise to significant environmental effects necessitating further documentation and analysis. This rule specifically addresses surface transportation cybersecurity as a standalone rule and is not part of a larger action.

Accordingly, this action is categorically excluded, and no further NEPA analysis or documentation is required. We seek any comments or information that may lead to the discovery of a significant environmental impact from this proposed rule.

F. Tribal consultation (E.O. 13175)

DHS analyzed this proposed rule under E.O. 13175 of November 6, 2000 (Consultation and Coordination with Indian Tribal Governments),[259] and determined that this rulemaking does not have tribal implications. For example, TSA determined that the applicability of requirements in proposed 49 CFR 1582.225 would not affect any public transportation systems owned or controlled by an Indian tribe, as defined in 24 U.S.C. 479A. Based on this determination, TSA has not specifically consulted with Indian tribal officials. Should TSA make a future determination that there is a risk to tribal owned/operated systems supporting the need for security enhancements, TSA will follow relevant consultation requirements before imposing any regulatory requirements.

List of Subjects

49 CFR Part 1500

Air carriers, Air transportation, Aircraft, Airports, Buses, Hazardous materials transportation, Law enforcement officers, Maritime carriers, Natural gas, Pipeline safety, Pipelines, Railroad safety, Railroads, Reporting and recordkeeping requirements, Security measures, Transportation facility, Vessels.

49 CFR Part 1503

Administrative practice and procedure, Investigations, Law enforcement, Penalties.

49 CFR Part 1520

Air carriers, Air transportation, Aircraft, Airports, Buses, Law enforcement officer, Maritime carriers, Railroad safety, Railroads, Reporting and recordkeeping

---

[259] Published at 65 FR 67249 (Nov. 9, 2000).

requirements, Security measures, Transportation facility, Vessels.

49 CFR Part 1570

Buses, Crime, Fraud, Hazardous materials transportation, Motor carriers, Railroads, Reporting and recordkeeping requirements, Security measures.

49 CFR Part 1580

Hazardous materials transportation, Railroad safety, Railroads, Reporting and recordkeeping requirements, Security measures.

49 CFR Part 1582

Mass transportation, Railroad safety, Railroads, Reporting and recordkeeping requirements, Security measures.

49 CFR Part 1584

Buses, Mass transportation, Reporting and recordkeeping requirements, Security measures.

49 CFR Part 1586

Gas, Hazardous materials transportation, Natural gas, Pipelines, Pipeline Safety, Reporting and recordkeeping requirements, Security measures.

The Proposed Amendments

For the reasons set forth in the preamble, the Transportation Security Administration is proposing to amend 49 CFR parts 1500, 1503, 1520, 1570, 1580, 1582, 1584, and 1586 to read as follows:

PART 1500—APPLICABILITY, TERMS, AND ABBREVIATIONS

1. Revise the authority citation for part 1500 to read as follows:

Authority: 49 U.S.C. 114, 5103, 40113, 44901-44907, 44912-44914, 44916-44918, 44935-44936, 44942, 46105; Pub. L. 110-53, 121 Stat. 266.

2. Amend § 1500.3 by:

a. Adding the definitions of “Carbon dioxide”, “Gas”, “Hazardous liquid”, “Liquefied natural gas (LNG)”, “Pipeline or pipeline system”, “Pipeline facility”, and

"TSA Cybersecurity Lexicon" in alphabetical order; and

b. Revising the definitions of "Transportation or transport", "Transportation facility", and "Transportation security equipment and systems".

The additions and revisions read as follows:

§ 1500.3 Terms and abbreviations used in this chapter.

* * * * *

Carbon dioxide means a fluid consisting of more than 90 percent carbon dioxide molecules compressed to a supercritical state.

* * * * *

Gas means natural gas, flammable gas, or gas which is toxic or corrosive.

* * * * *

Hazardous liquid means petroleum, petroleum products, anhydrous ammonia, and ethanol or other non-petroleum fuel, including biofuel, which is flammable, toxic, or would be harmful to the environment if released in significant quantities.

* * * * *

Liquefied natural gas (LNG) means natural gas or synthetic gas having methane (CH_4) as its major constituent that has been changed to a liquid.

* * * * *

Pipeline or Pipeline System means all parts of those physical facilities through which gas, hazardous liquid, carbon monoxide, or liquefied natural gas moves in transportation including, but not limited to pipe, line pipe, valves, and other appurtenance attached to pipe and line pipe, compressor units, metering stations, pumping units, regulator stations, metering stations, delivery stations, holders, fabricated assemblies, and breakout tanks as those terms are defined in 49 CFR parts 192, 193, and 195.

Pipeline facility means new or existing piping, pipes, pipelines, rights-of-way, and any equipment, facility, or building used in the treatment or transportation of gas,

hazardous liquid, carbon monoxide, or liquefied natural gas, as those terms are defined in 49 CFR parts 192, 193, and 195.

* * * * *

Transportation or *transport* means (1) the movement of property including loading, unloading, and storage; (2) the movement of people, boarding, and disembarking incident to that movement; and (3) the gathering, transmission, or distribution of gas or hazardous liquids by pipeline.

Transportation facility means a location at which transportation cargo, equipment or infrastructure assets are stored, equipment is transferred between conveyances and/or modes of transportation, transportation command and control operations are performed, or maintenance operations are performed. The term also includes, but is not limited to, passenger stations and terminals (including any fixed facility at which passengers are picked-up or discharged), vehicle storage buildings or yards, crew management centers, dispatching centers, fueling centers, telecommunication centers, and facilities used for the gathering, transmission, or distribution of gas or hazardous liquids by pipeline or the storage of gas or hazardous liquids.

Transportation security equipment and systems means items, both integrated into a system and stand-alone, used by owner/operators to enhance capabilities to detect, deter, prevent, or respond to a threat or incident, including, but not limited to, video surveillance, explosives detection, radiological detection, intrusion detection, Information Technology and Operational Technology authentication, network logging, motion detection, and security screening. This includes security equipment and systems for the protection and monitoring of both physical and logical/virtual assets.

* * * * *

TSA Cybersecurity Lexicon means a list of terms and their meaning applicable to cybersecurity requirements imposed by this chapter and available in a form and manner

determined by TSA. TSA may update and revise the lexicon following the procedures in this chapter for amendments to security programs.

* * * * *

PART 1503—INVESTIGATIVE AND ENFORCEMENT PROCEDURES

3. Revise the authority citation for part 1503 to read as follows:

Authority: 6 U.S.C. 1142; 18 U.S.C. 6002; 28 U.S.C. 2461 (note); 49 U.S.C. 114, 20109, 31105, 40113-40114, 40119, 44901-44907, 46101-46107, 46109-46110, 46301, 46305, 46311, 46313-46314; Pub. L. 104-134, 110 Stat. 1321, as amended by Pub. L. 114-74, 129 Stat. 584; Pub. L. 110-53, 121 Stat. 266.

PART 1520—PROTECTION OF SENSITIVE SECURITY INFORMATION

4. Revise the authority citation for part 1520 to read as follows:

Authority: 46 U.S.C. 114, 40113, 44901-44907, 44912-44914, 44916-44918, 44935-44936, 44942, 46105, 70102-70106, 70117; Pub. L. 110-53, 121 Stat. 266.

5. Amend § 1520.5 by revising paragraphs (b)(2)(i), (b)(3)(i), (b)(4)(i) and (ii), (b)(6)(ii), introductory text of (b)(12), (b)(13), and (b)(14) to read as follows:

§ 1520.5 Sensitive Security Information.

* * * * *

(b)* * *

(2) * * *

(i) Issued by TSA under 49 CFR 1542.303, 1544.305, 1548.19, 1570.201, or other authority;

* * * * *

(3) * * *

(i) Information circular issued by TSA under 49 CFR 1542.303, 1544.305, 1548.19, 1570.201, or other authority; and

* * * * *

(4) * * *

(i) Any device used by the Federal Government or any other person pursuant to any aviation, maritime, or surface transportation security requirements of Federal law for the detection of any person, and any weapon, explosive, incendiary, or destructive device, item, or substance; and

(ii) Any communications equipment used by the Federal government or any other person in carrying out or complying with any aviation, maritime, or surface transportation security requirements of Federal law.

* * * * *

(6) * * *

(ii) In the case of inspections or investigations performed by TSA, this includes the following information as to events that occurred within 12 months of the date of release of the information: the name of the airport or other transportation facility (including remote systems) where a violation occurred, the airport or other transportation facility identifier in the case number, a description of the violation, the regulation allegedly violated, and the identity of any operator in connection with specific locations or specific security procedures. Such information will be released after the relevant 12-month period, except that TSA will not release the specific gate or other location on an airport or other transportation facility where an event occurred, regardless of the amount of time that has passed since its occurrence. During the period within 12 months of the date of release of the information, TSA may release summaries of an operator's, but not an airport operator's, total security violations in a specified time range without identifying specific violations or locations. Summaries may include total enforcement actions, total proposed civil penalty amounts, number of cases opened, number of cases referred to TSA or FAA counsel for legal enforcement action, and number of cases closed.

* * * * *

(12) *Critical transportation infrastructure asset information.* Any list identifying systems or assets, whether physical or logical/virtual, so vital to the aviation, maritime, or surface transportation that the incapacity or destruction of such assets would have a debilitating impact on transportation security, if the list is—

* * * * *

(13) *Systems security information.* Any information involving the security of operational or administrative data systems operated by the Federal government that have been identified by the DOT or DHS as critical to aviation, maritime, or surface transportation safety or security, including automated information security procedures and systems, security inspections, and vulnerability information concerning those systems.

(14) *Confidential business information.* (i) Solicited or unsolicited proposals received by DHS or DOT, and negotiations arising therefrom, to perform work pursuant to a grant, contract, cooperative agreement, or other transaction, but only to the extent that the subject matter of the proposal relates to aviation, maritime, or surface transportation security measures;

(ii) Trade secret information, including information required or requested by regulation or SD, obtained by DHS or DOT in carrying out aviation, maritime, or surface transportation security responsibilities; and

(iii) Commercial or financial information, including information required or requested by regulation or SD, obtained by DHS or DOT in carrying out aviation, maritime, or surface transportation security responsibilities, but only if the source of the information does not customarily disclose it to the public.

* * * * *

6. Amend § 1520.7 by revising paragraph (i) to read as follows:

§ 1520.7 Covered persons.

* * * * *

(i) Each person conducting research and development activities that relate to aviation, maritime, or surface transportation security and are approved, accepted, funded, recommended, or directed by DHS or DOT.

* * * * *

PART 1570—GENERAL RULES

7. Revise the authority citation for part 1570 to read as follows:

Authority: 18 U.S.C. 842, 845; 46 U.S.C. 70105; 49 U.S.C. 114, 5103a, 40113, and 46105; Pub. L. 108-90, 117 Stat. 1156, as amended by Pub. L. 110-329, 122 Stat. 3689; Pub. L. 110-53, 121 Stat. 266.

Subpart A—General

8. Revise § 1570.1 to read as follows:

§ 1570.1 Scope.

(a) *Applicability.* This part applies to any person involved in maritime or surface transportation as specified in this subchapter.

(b) *Delegation of authority*. (1) Where the Administrator is named in this subchapter as exercising authority over a function, the authority is exercised by the Administrator or the Deputy Administrator, or any individual formally designated to act as the Administrator or the Deputy Administrator.

(2) Where TSA or the designated official is named in this subchapter as exercising authority over a function, the authority is exercised by the official designated by the Administrator to perform that function.

9. Amend § 1570.3 by adding the definitions “Accountable executive”, “Cybersecurity”, “Cybersecurity-sensitive employee”, and “Physical security” in alphabetical order to read as follows:

§ 1570.3 Terms used in this subchapter.

* * * * *

Accountable executive means an individual identified by an owner/operator who has responsibility and accountability for the owner/operator's compliance with the requirements of this subchapter, including authority over human resource issues, major financial issues, conduct of the owner/operator's affairs, all operations conducted related to the requirements of this subchapter, and responsibility for all transportation-related security issues.

* * * * *

Cybersecurity means measures to prevent damage to, protect, and restore Information Technology and Operational Technology systems as defined in the TSA Cybersecurity Lexicon, including protection of data to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. Cybersecurity and physical security are not mutually exclusive concepts.

Cybersecurity-sensitive employee means any employee who is a privileged user with access to, or privileges to access, a Critical Cyber System or any Information or Operational Technology system that is interdependent with a Critical Cyber System as defined in the TSA Cybersecurity Lexicon.

* * * * *

Physical security means measures to (1) protect the safety and security of persons and property resulting from disruption of operations; (2) prevent damage to, protection of, and restoration of physical assets and operations; and (3) controls to prevent unauthorized access to or disruption of physical and virtual assets and operations. Physical security encompasses the security of systems and facilities, as well as the persons in areas in or near to operations that could have their safety and security threatened by an attack on physical systems and assets. Cybersecurity and physical security are not mutually exclusive concepts.

* * * * *

10. Amend § 1570.7 by adding paragraph (a)(4) to read as follows:

§ 1570.7 Security responsibilities of employees and other persons.

(a) * * *

(4) Access information or operational technology systems without complying with the security measures required under this subchapter to control access to or modification to such systems.

* * * * *

11. Revise subpart B of part 1570 to read as follows:

Subpart B—Security Programs

Sec.

1570.101 Scope.
1570.103 Content.
1570.105 Responsibility for determinations.
1570.107 Approval and amendments.
1570.109 Alternate means of compliance for seasonal or infrequent operations.
1570.111 Extensions of time.
1570.113 [Reserved]
1570.115 Withdrawal of approval of a security program.
1570.117 Recordkeeping and availability.
1572.119 Exhaustion of administrative remedies.
1570.121 Severability.

§ 1570.101 Scope.

The requirements of this subpart address general security program requirements applicable to each owner/operator required to have a security program under parts 1580, 1582, 1584, and 1586 of this subchapter.

§ 1570.103 Content.

(a) *Security program.* Except as otherwise approved by TSA, each owner/operator required to have a security program under parts 1580, 1582, 1584, or 1586 of this subchapter must include in its security program detailed information describing how it addresses each of the requirements identified in the applicable part.

(b) *Index.* The owner/operator required to have a security program under parts 1580, 1582, 1584, or 1586 of this subchapter must ensure the required security program

includes an index organized in the same subject area sequence as the requirements in the applicable part or subpart.

(c) *Use of appendices.* (1) The owner/operator may comply with the requirement in paragraph (a) of this section by including in its security program any document that contains the information required by the applicable security program required by parts 1580, 1582, 1584, or 1586 of this subchapter, including previously developed plans, policies, and /or procedures that support compliance with these requirements.

(2) These documents may be provided as either an appendix to the security program or as a list of documents, including specific applicable sections, that contain the required information. The owner/operator must include an index of the records and their location organized in the same sequence as the requirements in the applicable parts.

(3) The appendix or documents listed in it must be explicitly incorporated by reference and become part of the corresponding section(s) of the security program.

§ 1570.105 Responsibility for determinations.

(a) *Higher-risk operations.* Owner/operators of freight railroads, public transportation systems, passenger railroads, over-the-road buses (OTRB), and pipeline system and facilities are required to determine if the applicability criteria identified for security programs or other requirements identified in parts 1580, 1582, 1584, or 1586 of this subchapter apply to their operations. Unless otherwise notified in writing by TSA, owner/operators must notify TSA of applicability before [DATE 30 DAYS AFTER EFFECTIVE DATE OF FINAL RULE].

(b) *New or modified operations.* If an owner/operator commences new operations or modifies existing operations after [DATE 30 DAYS AFTER EFFECTIVE DATE OF FINAL RULE], that owner/operator is responsible for determining whether the new or modified operations would meet the applicability criteria in parts 1580, 1582, 1584, or 1586 of this subchapter and must notify TSA no more than the later of [DATE 60 DAYS

AFTER EFFECTIVE DATE OF FINAL RULE] or 60 calendar days before commencing operations or implementing modifications that would result in meeting the applicability criteria.

(c) *Continued applicability.* Once an owner/operator becomes subject to the requirements in parts 1580, 1582, 1584, or 1586 of this subchapter, the requirements continue to apply unless otherwise exempted under the procedures in paragraph (d) of this section.

(d) *Permanent changes in operations.* If an owner/operator changes operations to the extent that any of the applicability criteria for requirements in parts 1580, 1582, 1584, or 1586 of this subchapter no longer apply, the owner/operator is responsible for notifying TSA of the change. Notification must be provided in writing and include documentation that operations no longer meet the criteria for applicability. TSA may require additional documentation to support the owner/operator's assertions. If TSA confirms the change in operations, TSA will provide a written, operation and requirement-specific exemption to the owner/operator. If the operations change in the future, the owner/operator must comply with the procedures in paragraph (b) for new or modified operations.

§ 1570.107 Approval and amendments.

(a) *Initial approval of security program.* Unless otherwise authorized by TSA, each owner/operator required to have a security program under this subchapter must submit its proposed security program to TSA for approval no later than the deadline specified in the applicable requirements. The proposed security program must meet the requirements applicable to its operation, as required by this subchapter. The following procedures apply to security program approvals:

(1) *TSA approval.* Within 60 days of receiving the owner/operator's proposed security program required by parts 1580, 1582, 1584, or 1586 of this subchapter, the

designated official will either approve the program or give the owner/operator written notice to modify the program to comply with the applicable requirements of this subchapter. TSA may request additional information, and the owner/operator must provide the information within the time period TSA prescribes. The 60-day period for TSA approval will begin when the owner/operator provides the additional information. After all required information is received, TSA will notify the owner/operator if it needs an extension of time to approve the program or provide the owner/operator with written notice to modify the program to comply with the applicable requirements of this subchapter.

(2) *Notice to modify.* (i) If TSA provides the owner/operator with written notice to modify the security program to comply with the applicable requirements of this subchapter, the owner/operator must provide a modified security program to TSA for approval within the timeframe specified by TSA.

(ii) The owner/operator may either submit a modified security program to the designated official for approval, or petition for reconsideration under paragraph (f) of this section within 30 days of receiving a notice to modify.

(b) *Amendment requested by an owner/operator.* Once a security program (including any appendices, policies, procedures, or measures incorporated by reference) required by parts 1580, 1582, 1584, or 1586 is approved by TSA, the owner/operator must request an amendment for any permanent (intended to be in effect for 60 or more calendar days), substantive changes to its security program. Except as provided in paragraph (c), an owner/operator requesting approval to amend its security program must request an amendment in advance of implementing the proposed change using the following procedures:

(1) The request for an amendment must be filed with the designated official at least 45 days before the date it proposes for the amendment to become effective unless a

shorter period is allowed by the designated official.

(2) Within 30 days after receiving a proposed amendment, the designated official, in writing, either approves or denies the request to amend.

(3) TSA may approve an amendment to a security program if the designated official determines that the interest of the public and transportation security will allow it, and the proposed amendment provides the level of security required under this subchapter. In considering the request for alternative measures, TSA will review all relevant factors including—

(i) The risks associated with the type of operation, for example, whether the owner/operator transports hazardous materials or passengers within a high threat urban area, whether the owner/operator transports passengers and the volume of passengers transported, or whether the owner/operator hosts a passenger operation.

(ii) Any relevant threat information.

(iii) Other circumstances concerning potential risk to the public and transportation security.

(4) No later than 30 calendar days after receiving a denial, the owner/operator may petition for reconsideration under paragraph (e) of this section.

(5) Owner/operators may submit a group proposal for an amendment that is on behalf of it and other owner/operators that co-sign the proposal. The joint proposal may only be submitted by owner/operators subject to the applicable requirements.

(c) *Administrative, clerical, and temporary changes to policies, procedures, or measures in a TSA-approved Security Program.*

(1) *Administrative or clerical changes.* (i) An owner/operator is not required to notify TSA of administrative or technical changes to its TSA-approved security program. This exception is limited to changes that do not affect policies, procedures, or measures in the owner/operator's TSA-approved security program.

(ii) Owner/operators must keep a chronological record of administrative or clerical changes that indicates the relevant portion of the security program that is being changed and when the change occurred. This information must be maintained for a duration that includes, at a minimum, any changes made during the period of one year before the date of the most recently approved security program.

(2) *Temporary changes affecting security matters.* (i) The owner/operator must notify TSA in writing no more than 24 hours after any temporary, substantive change to its TSA-approved security program. For purposes of this requirement, a temporary, substantive change is any change that affects policies, procedures, or measures in the owner/operator's TSA-approved security program, that is not intended to be in effect for 60 or more calendar days.

(ii) Within seven calendar days of the notification in paragraph (c)(2)(i), the owner/operator must inform TSA, in writing, of each interim policy, procedure, or measure being used to maintain adequate security while the temporary, substantive change is in effect. The owner/operator must include in its written notification a description of how the interim policy, procedure, or measure provides the same level of security as the previously approved policy, procedure, or measure. TSA will notify the owner/operator in writing if TSA does not concur that the interim measures provide a commensurate level of security. TSA may request additional information to make its determination.

(iii) If the duration of the temporary, substantive change exceeds or is expected to exceed 60 or more calendar days, the owner/operator must seek an amendment to the security program as required by paragraph (b). The request for an amendment must be submitted no more than 65 days after the temporary, substantive change initially took effect.

(d) *Amendment by TSA.* In the interest of the public and transportation security,

TSA may amend a security program using the following procedures:

(1) The designated official will notify the owner/operator, in writing, of the proposed amendment, fixing a period of not less than 30 calendar days within which the owner/operator may submit written information, views, and arguments on the amendment.

(2) After considering all relevant material, the designated official will notify the owner/operator of any amendment adopted or rescind the notice of amendment. If the amendment is adopted, it becomes effective not less than 30 calendar days after the owner/operator receives the notice of amendment, unless the owner/operator submits a petition for reconsideration under paragraph (f) of this section no later than 15 calendar days before the effective date of the amendment. A timely petition for reconsideration stays the effective date of the amendment.

(e) *Emergency amendments.* If the designated official finds that there is an emergency requiring immediate action to protect transportation security that makes procedures in this section contrary to the public interest, the designated official may issue an amendment, without the prior notice and comment procedures in paragraph (c) of this section, effective without stay on the date the owner/operator receives notice of it. In such a case, the designated official will incorporate in the notice a brief statement of the reasons and findings for the amendment to be adopted. The owner/operator may file a petition for reconsideration under paragraph (e) of this section within 15 calendar days of the effective date of the emergency amendment; however, this filing does not stay the effective date of the emergency amendment.

(f) *Petitions for reconsideration.* (1) *Process for filing.* If an owner/operator seeks to petition for reconsideration of a determination, required modification, denial of a request for an amendment by the owner/operator, denial to rescind a TSA-required amendment, denial of an alternative measure, or issuance of a security directive, the

owner/operator must submit the petition, together with any pertinent information, to the Administrator for reconsideration. The petition for reconsideration must be submitted within the timeframe given in the applicable section and include a statement and any supporting documentation explaining why the owner/operator believes TSA's decision or action is incorrect. TSA review of a petition for reconsideration will begin when the owner/operator provides all required information.

(2) *TSA review.* Upon review of the petition for reconsideration, the Administrator or designee will dispose of the petition for reconsideration by affirming, modifying, or rescinding its previous decision.

(3) *Final agency action.* The disposition of a petition for reconsideration by the Administrator is considered a final agency action.

§ 1570.109 Alternate means of compliance for seasonal or infrequent operations.

If in TSA's judgment, the overall safety and security of operations for which a security program is required under this subchapter are not diminished, then TSA may approve a security program that provides for the use of alternate measures. Such a program may be considered only for an owner/operator at which operations that meet the criteria for applicability in parts 1580, 1582, 1584, or 1586 of this subchapter are determined by TSA to be seasonal or infrequent.

§ 1570.111 Extensions of time.

TSA may grant an extension of time for implementing a security program required by this subchapter upon a showing of good cause. The owner/operator must request the extension of time in writing, and TSA must receive the request within a reasonable time before the due date to be extended; an owner/operator may request an extension after the expiration of a due date by sending a written request describing why the failure to meet the due date was excusable. TSA will respond to the request in writing.

§ 1570.113 [Reserved]

§ 1570.115 Withdrawal of approval of a security program.

(a) *Applicability.* This section applies to holders of a security program approved or accepted by TSA under 49 CFR chapter XII, subchapter D.

(b) *Withdrawal of security program approval.* TSA may withdraw the approval of a security program, if TSA determines continued operation is contrary to security and the public interest, as follows:

(1) *Notice of proposed withdrawal of approval.* TSA will serve a Notice of Proposed Withdrawal of Approval, which notifies the holder of the security program, in writing, of the facts, charges, and applicable law, regulation, or order that form the basis of the determination.

(2) *Security program holder's reply.* The holder of the security program may respond to the Notice of Proposed Withdrawal of Approval no later than 15 calendar days after receipt of the withdrawal by providing the designated official, in writing, with any material facts, arguments, applicable law, and regulation.

(3) *TSA review.* The designated official will consider all information available, including any relevant material or information submitted by the holder of the security program, before either issuing a Withdrawal of Approval of the security program or rescinding the Notice of Proposed Withdrawal of Approval. If TSA issues a Withdrawal of Approval, it becomes effective upon receipt by the holder of the security program, or 15 calendar days after service, whichever occurs first.

(4) *Petition for reconsideration.* The holder of the security program may petition TSA to reconsider its Withdrawal of Approval by serving a petition for consideration no later than 15 calendar days after the holder of the security program receives the Withdrawal of Approval. The holder of the security program must serve the Petition for Reconsideration on the designated official. Submission of a Petition for Reconsideration

will not stay the Withdrawal of Approval. The holder of the security program may request the designated official to stay the Withdrawal of Approval pending review of and decision on the Petition.

(5) *Administrator's review.* The designated official transmits the Petition together with all pertinent information to the Administrator for reconsideration. The Administrator will dispose of the Petition within 15 calendar days of receipt by either directing the designated official to rescind the Withdrawal of Approval or by affirming the Withdrawal of Approval. The decision of the Administrator constitutes a final agency order subject to judicial review in accordance with 49 U.S.C. 46110.

(6) *Emergency withdrawal.* If TSA finds that there is an emergency with respect to transportation security requiring immediate action that makes the procedures in this section contrary to the public interest, the designated official may issue an Emergency Withdrawal of Approval of a security program without first issuing a Notice of Proposed Withdrawal of Approval. The Emergency Withdrawal would be effective on the date that the holder of the security program receives the emergency withdrawal. In such a case, the designated official will send the holder of the security program a brief statement of the facts, charges, applicable law, regulation, or order that forms the basis for the Emergency Withdrawal. The holder of the security program may submit a Petition for Reconsideration under the procedures in paragraphs (b)(4) through (b)(5) of this section; however, this petition will not stay the effective date of the Emergency Withdrawal.

(c) *Service of documents for withdrawal of approval of security program proceedings.* Service may be accomplished by personal delivery, certified mail, or express courier. Documents served on the holder of a security program will be served at its official place of business as designated in its security program. Documents served on TSA must be served to the address noted in the Notice of Withdrawal of Approval or Withdrawal of Approval, whichever is applicable.

(1) *Certificate of service.* An individual may attach a certificate of service to a document tendered for filing. A certificate of service must consist of a statement, dated and signed by the person filing the document, that the document was personally delivered, served by certified mail on a specific date, or served by express courier on a specific date.

(2) *Date of service.* The date of service is—

(i) The date of personal delivery;

(ii) If served by certified mail, the mailing date shown on the certificate of service, the date shown on the postmark if there is no certificate of service, or other mailing date shown by other evidence if there is no certificate of service or postmark; or

(iii) If served by express courier, the service date shown on the certificate of service, or by other evidence if there is no certificate of service.

(d) *Extension of time.* TSA may grant an extension of time to the limits set forth in this section for good cause shown. A security program holder must submit a request for an extension of time in writing, and TSA must receive it at least 2 days before the due date to be considered. TSA may grant itself an extension of time for good cause.

§ 1570.117 Recordkeeping and availability.

(a) *Retention.* In addition to submission of documents as required by parts 1580, 1582, 1584, and 1586 of this subchapter, each owner/operator required to have a security program under these parts must—

(1) Maintain and make available to TSA records to establish compliance with the requirements in this subchapter, including all plans, procedures, and other documents (including cited sections of these documents) incorporated by reference into a security program required by parts 1580, 1582, 1584, or 1586 of this subchapter.

(2) [Reserved]

(b) *Location.* The records required by paragraph (a) of this section must be

retained at the owner/operator's corporate headquarters unless otherwise directed by TSA.

(c) *Physical and electronic records.* (1) Except as provided in paragraph (c)(2), each owner/operator required to retain records under this section may keep them in electronic form. An owner/operator may maintain and transfer records through electronic transmission, storage, and retrieval provided that the electronic system provides for the maintenance of records as originally submitted without corruption, loss of data, or tampering.

(2) The owner/operator must maintain one written copy of the current and complete TSA-approved security program required by the applicable part or subpart of this subchapter, signed by the owner/operator, at its corporate headquarters, plus one written copy of the most recent security program previously approved by TSA.

(d) *Availability to TSA.* Each owner/operator must make the records available to TSA upon request, including through electronic submission if applicable, for inspection and copying.

(e) *Protection of SSI.* Each owner/operator must restrict the distribution, disclosure, and availability of Sensitive Security Information, as identified in part 1520 of this chapter, to persons with a need to know. The owner/operator must refer requests for such information by other persons to TSA.

(f) *Dissemination to employees*. Subject to the restrictions in paragraph (e) of this section, each owner/operator must make copies of the security program, relevant portions of the security program, or implementing instructions available to the employees who are responsible for implementing it, consistent with personnel security access rights, background investigation restrictions, and a demonstrated need to know.

§ 1570.119 Exhaustion of administrative remedies.

Persons subject to the requirements in parts 1570, 1580, 1582, 1584, and 1586 of

this subchapter must exhaust the administrative remedies set forth in this part before seeking judicial review.

§ 1570.121 Severability.

Any provision of this subchapter held to be invalid or unenforceable as applied to any person or circumstance shall be construed so as to continue to give the maximum effect to the provision permitted by law, including as applied to persons not similarly situated or to dissimilar circumstances, unless such holding is that the provision of this subchapter is invalid and unenforceable in all circumstances, in which event the provision shall be severable from the remainder of this subchapter and shall not affect the remainder thereof.

12. Revise subpart C of part 1570 to read as follows:

Subpart C—Threat and Threat Response

Sec.

1570.201 Security Directives and Information Circulars.
1570.203 Alternate measures.

§ 1570.201 Security Directives and Information Circulars.

(a) The requirements in this section apply to each owner/operator identified in §§ 1580.1, 1582.1, 1584.1, and 1586.1 of this subchapter.

(b) TSA may issue an Information Circular to notify owner/operators of security concerns. When TSA determines that additional security measures are necessary to respond to a threat assessment or to a specific threat against transportation security, TSA issues a Security Directive setting forth mandatory measures.

(c) Each owner/operator must comply with each Security Directive issued to the owner/operator within the time prescribed in the Security Directive.

(d) Each owner/operator that receives a Security Directive must—

(1) Within the time prescribed in the Security Directive, acknowledge receipt of the Security Directive to TSA as required in the Security Directive.

(2) Within the time prescribed in the Security Directive, specify the method by which the measures in the Security Directive have been implemented (or will be implemented, if the Security Directive is not yet effective).

(e) In the event that the owner/operator is unable to implement the measures in the Security Directive, the owner/operator must submit proposed alternative measures following the procedures in § 1570.203, and the basis for submitting the alternative measures to TSA for approval. The owner/operator must implement any alternative measures approved by TSA.

(f) Each owner/operator that receives a Security Directive may comment on the Security Directive by submitting data, views, or arguments in writing to TSA. TSA may amend the Security Directive based on comments received. Submission of a comment does not delay the effective date of the Security Directive.

(g) The owner/operator may file a petition for reconsideration under paragraph (e) of § 1570.107 within 15 days of the effective date of a Security Directive; however, this filing does not stay the effective date of the Security Directive.

(h) Except as provided in paragraph (h)(3) of this section, each owner/operator that receives a Security Directive or an Information Circular and each person who receives information from a Security Directive or an Information Circular must:

(1) Restrict the availability of the Security Directive or Information Circular, and information contained in either document, to those persons with an operational need-to-know.

(2) Refuse to release the Security Directive or Information Circular, and information contained in either document, to persons other than those who have an operational need to know without the prior written consent of TSA.

(3) The requirements in paragraph (h)(1) and (h)(2) of this section do not apply if the TSA Administrator, or designee, under the authority of § 1520.5(c) of this chapter,

determines that a Security Directive or Information Circular does not contain Sensitive Security Information.

§ 1570.203 Alternative measures.

(a) If in TSA's judgment, the overall security of transportation provided by an owner/operator subject to the requirements of parts 1580, 1582, 1584, or 1586 of this subchapter are not diminished, TSA may approve alternative measures to requirements in a Security Directive.

(b) Each owner/operator requesting alternative measures must file the request for approval in a form and manner prescribed by TSA. The filing of such a request does not affect the owner/operator's responsibility for compliance while the request is being considered.

(c) TSA may request additional information, and the owner/operator must provide the information within the period TSA prescribes. Within 30 calendar days after receiving a request for alternative measures and all requested information, TSA will, in writing, either approve or deny the request.

(d) If TSA finds that the use of the alternative measures is in the interest of the public and transportation security, it may grant the request subject to any conditions TSA deems necessary. In considering the request for alternative measures, TSA will review all relevant factors, including—

(1) The risks associated with the type of operation, for example, whether the owner/operator transports hazardous materials or passengers within a high threat urban area, whether the owner/operator transports passengers and the volume of passengers transported, or whether the owner/operator hosts a passenger operation.

(2) Any relevant threat information.

(3) Other circumstances concerning potential risk to the public and transportation security.

(e) No later than 30 calendar days after receiving a denial, the owner/operator may petition for reconsideration under § 1570.107(f).

Appendix A to Part 1570 [Removed]

13. Remove Appendix A to part 1570.

PART 1580—FREIGHT RAIL TRANSPORTATION SECURITY

14. The authority citation for part 1580 continues to read as follows:

Authority: 49 U.S.C. 114; Pub. L. 110-53 (121 Stat. 266, Aug. 3, 2007) secs. 1501 (6 U.S.C. 1151), 1512 (6 U.S.C. 1162) and 1517 (6 U.S.C. 1167).

Subpart A—General

15. Amend § 1580.3 by:

a. Revising the introductory paragraph;

b. Removing the definition of "Class I";

c. Adding the definitions of "Class I, II, or III", "Component", "Defense Connector Railroad", "Positive Train Control", "Switching or terminal service", and "Train miles" in alphabetical order.

The revision and additions read as follows:

§ 1580.3 Terms used in this part.

In addition to the terms in §§ 1500.3, 1500.5, and 1503.103 of subchapter A and § 1570.3 of subchapter D of this chapter, the following terms apply to this part:

* * * * *

Class I, Class II, or Class III freight railroad has the same meaning as "Class I," "Class II," and "Class III" freight railroads as determined by regulations of the Surface Transportation Board c).

Component has the same meaning as "component" as defined in 49 CFR 236.903.

Defense Connector Railroad means a railroad that has a line of common carrier obligation designated a defense connector line by the US Army Military Surface

Deployment and Distribution Command Transportation Engineering Agency (SDDCTEA) and Federal Railroad Administration (FRA) which connects defense installations or other activities requiring rail service to the Strategic Rail Corridor Network (STRACNET).

* * * * *

Positive train control (PTC) has the same meaning as "positive train control" as defined in 49 CFR 236.1003.

* * * * *

Switching or terminal services means the furnishing or terminal facilities for passenger or freight rail traffic for line-haul service and the movement of railroad cars between terminal yards, industrial sidings, and other local sites. This term does not include movement of a train or part of a train within yard limits by the road locomotive and the placement of locomotives or cars in a train or their removal from a train by the road locomotive while en route to the train's destination.

Train miles means a unit in railroad accounting that refers to the distance of one mile covered by a single train, which may have several cars.

16. Revise subpart B of part 1580 to read as follows:

Subpart B—Security Programs: Physical Security

Sec.

1580.101 Scope.
1580.103 Physical Security Coordinator.
1580.105 Reporting of significant physical security concerns.
1580.107 [Reserved]
1580.109 [Reserved]
1580.111 [Reserved]
1580.113 Security training program requirements.
1580.115 [Reserved]

§ 1580.101 Scope.

This subpart includes requirements that are primarily intended to ensure the physical security of freight rail operations. Physical security encompasses the security of

individuals, cargo, rail secure areas, rail cars, and transportation facilities, as well as the persons in areas in or near to rail operations that could have their safety and security threatened by an attack on physical systems and assets. Each person identified in § 1580.1 must review the applicability in each section of this subpart to determine whether they are an owner/operator to whom the requirements apply based on their operations and the criteria for applicability.

§ 1580.103 Physical Security Coordinator.

(a) (1) Except as provided in paragraph (a)(2) of this section, each owner/operator identified in § 1580.1 must designate and use a primary and at least one alternate Physical Security Coordinator at the corporate level to function as the administrator for sharing security-related activities and information.

(2) An owner/operator identified in § 1580.1(a)(5) (private rail cars and circus trains) must designate and use a primary and at least one alternate Physical Security Coordinator, only if notified by TSA in writing that a threat exists concerning that type of operation.

(b) The primary Physical Security Coordinator and alternate(s) must—

(1) Be accessible to TSA on a 24 hours per day, 7 days per week basis;

(2) Serve as the primary contact(s) for intelligence information and security-related activities and communications with TSA. Any individual designated as a Physical Security Coordinator may perform other duties in addition to the duties described in this section; and

(3) Coordinate security practices and procedures required by this subchapter internally and with appropriate law enforcement and emergency response agencies.

(c) The Physical Security Coordinator and alternate(s) must be a U.S. citizen eligible for a security clearance, unless otherwise waived by TSA.

(d) Each owner/operator required to have a Physical Security Coordinator must

provide in writing to TSA the names, U.S. citizenship status, titles, business phone number(s), and business email address(es) of the Physical Security Coordinator and alternate(s). Changes in any of the information required by this section must be submitted to TSA within 7 calendar days.

§ 1580.105 Reporting of significant physical security concerns.

(a) Each owner/operator identified in § 1580.1 must report, within 24 hours of initial discovery, any potential threats and significant physical security concerns involving transportation-related operations in the United States or transportation to, from, or within the United States as soon as possible by the methods prescribed by TSA.

(b) Potential threats or significant physical security concerns encompass incidents, suspicious activities, and threat information affecting physical operations including, but not limited to, the categories of reportable events listed in appendix C to this part.

(c) Information reported must include the following, as available and applicable:

(1) The name of the reporting individual and contact information, including a telephone number or email address.

(2) The affected freight or passenger train, station, terminal, rail hazardous materials facility, or other transportation facility or infrastructure, including identifying information and current location.

(3) Scheduled origination and termination locations for the affected freight or passenger train−including departure and destination city and route.

(4) Description of the threat, incident, or activity, including who has been notified and what action has been taken.

(5) The names, other available biographical data, and/or descriptions (including vehicle or license plate information) of individuals or motor vehicles known or suspected to be involved in the threat, incident, or activity.

(6) The source of any threat information.

§ 1580.107 [Reserved]

§ 1580.109 [Reserved]

§ 1580.111 [Reserved]

§ 1580.113 Security training program requirements.

(a) *Applicability.* This section applies to each owner/operator—

(1) Described in § 1580.1(a)(1) that is a Class I freight railroad.

(2) Described in § 1580.1(a)(1) that transports one or more of the categories and quantities of RSSM in an HTUA.

(3) Described in § 1580.1(a)(4) that serves as a host railroad to a freight railroad described in paragraphs (a)(1) or (a)(2) or a passenger operation described in § 1582.101 of this subchapter.

(b) *Training required for security-sensitive employees.* No owner/operator identified in paragraph (a) of this section may use a security-sensitive employee to perform a function identified in Appendix B to this part, unless that individual has received training as part of a security training program approved by TSA or is under the direct supervision of an employee who has received the training required by this section as applicable to that security-sensitive function. Upon approval, this security training program becomes part of the owner/operators TSA-approved security program.

(c) *Limits on use of untrained employees.* Notwithstanding paragraph (b) of this section, a security-sensitive employee may not perform a security-sensitive function for more than 60 calendar days without receiving security training.

(d) *General requirements.* Each owner/operator required to provide security training to its employees under this section must submit its security training program to TSA for approval in a form and manner prescribed by TSA. The security training program must include the following information:

(1) Name of owner/operator.

(2) Name, title, telephone number, and email address of the primary individual to be contacted about review of the security training program.

(3) Number, by specific job function category identified in Appendix B to this part, of security-sensitive employees trained or to be trained.

(4) Implementation schedule that identifies a specific date by which the required initial and recurrent security training will be completed.

(5) Location where training program records will be maintained.

(6) Plan for ensuring supervision of untrained security-sensitive employees performing functions identified in Appendix B to this part.

(7) Plan for notifying employees of changes to security measures that could change information provided in previously provided training.

(8) Method(s) for evaluating the effectiveness of the security training program in each area required by paragraph (e) of this section.

(e) *General curriculum requirements.* The security training program submitted to TSA for approval must include a curriculum or lesson plan, including learning objectives and method of delivery (such as instructor-led or computer-based training) for each course used to meet the requirements in paragraph (f) of this section. TSA may request additional information regarding the curriculum during the review and approval process. If recurrent training under paragraph (j) of this section is not the same as initial training, a curriculum or lesson plan for the recurrent training must be submitted and approved by TSA.

(f) *Specific curriculum requirements.* (1) *Prepare.* Each owner/operator must ensure that each of its security-sensitive employees with position- or function-specific responsibilities under the owner/operator's security program has knowledge of how to fulfill those responsibilities in the event of a security threat, breach, or incident to ensure—

(i) Employees with responsibility for transportation security equipment and systems are aware of their responsibilities and can verify the equipment and systems are operating and properly maintained; and

(ii) Employees with other duties and responsibilities under the company's security plans and/or programs, including those required by Federal law, know their assignments and the steps or resources needed to fulfill them.

(2) *Chain of Custody.* Each employee who performs any security-related functions under § 1580.205 of this subchapter must be provided training specifically applicable to the functions the employee performs. As applicable, this training must address—

(i) Inspecting rail cars for signs of tampering or compromise, IEDs, suspicious items, and items that do not belong;

(ii) Identification of rail cars that contain rail security-sensitive materials, including the owner/operator's procedures for identifying rail security-sensitive material cars on train documents, shipping papers, and in computer train/car management systems; and

(iii) Procedures for completing transfer of custody documentation.

(3) *Observe.* Each owner/operator must ensure that each of its security-sensitive employees has knowledge of the observational skills necessary to recognize—

(i) Suspicious and/or dangerous items, such as substances, packages, or conditions (for example, characteristics of an Improvised Explosive Device and signs of equipment tampering or sabotage);

(ii) Combinations of actions and individual behaviors that appear suspicious and/or dangerous, inappropriate, inconsistent, or out of the ordinary for the employee's work environment, which could indicate a threat to transportation security; and

(iii) How a terrorist or someone with malicious intent may attempt to gain

sensitive information or take advantage of vulnerabilities.

(4) *Assess.* Each owner/operator must ensure that each of its security-sensitive employees has knowledge necessary to—

(i) Determine whether the item, individual, behavior, or situation requires a response as a potential terrorist threat based on the respective transportation environment; and

(ii) Identify appropriate responses based on observations and context.

(4) *Respond.* Each owner/operator must ensure that each of its security-sensitive employees has knowledge of how to—

(i) Appropriately report a security threat, including knowing how and when to report internally to other employees, supervisors, or management, and externally to Local, State, or Federal agencies according to the owner/operator's security procedures or other relevant plans;

(ii) Interact with the public and first responders at the scene of the threat or incident, including communication with passengers on evacuation and any specific procedures for individuals with disabilities and the elderly; and

(iii) Use any applicable self-defense devices or other protective equipment provided to employees by the owner/operator.

(g) *Relation to other training.* Training conducted by owner/operators to comply with other requirements or standards, such as emergency preparedness training required by the Department of Transportation (DOT) (49 CFR part 239) or other training for communicating with emergency responders to arrange the evacuation of passengers, may be combined with, and used to satisfy, elements of the training requirements in this section.

(h) *Submission.* If commencing or modifying operations subject to these requirements after June 21, 2021, the training program must be submitted to TSA no later

than 90 calendar days before commencing new or modified operations.

(i) *Initial security training.* Each owner/operator must provide initial security training to security-sensitive employees, using the curriculum approved by TSA and in compliance with the following schedule. (1) For security training programs submitted to TSA for approval after March 22, 2021, if the employee is employed to perform a security-sensitive function on the date TSA approves the program, then initial training must be provided no later than 12 months after the date that TSA approves the owner/operator's security training program.

(2) If performance of a security-sensitive job function is initiated after TSA approves the owner/operator's security training program, then initial training must be provided no later than 60 calendar days after the employee first performs the security-sensitive job function.

(3) If the security-sensitive job function is performed intermittently, then initial security training must be provided no later than the 60th calendar day of employment performing a security-sensitive function, aggregated over a consecutive 12-month period.

(j) *Recurrent security training.* (1) Except as provided in paragraph (j)(2) of this section, a security-sensitive employee required to receive training must receive the required training at least once every 3 years.

(2) If an owner/operator modifies a security program or security plan for which training is required, the owner/operator must ensure each security-sensitive employee with position- or function-specific responsibilities related to the revised plan or program changes receives training on the revisions within 90 days of implementation of the revised plan or program changes. All other employees must receive training that reflects the changes to the operating security requirements as part of their regularly scheduled recurrent training.

(3) The 3-year recurrent training cycle is based on the anniversary calendar month

of the employee's initial security training. If the owner/operator provides the recurrent security training in the month of, the month before, or the month after it is due, the employee is considered to have taken the training in the month it is due.

(k) *Recognition of prior training.* Previously provided security training may be credited towards satisfying the requirements of this section provided the owner/operator—

(1) Obtains a complete record of such training and validates the training meets requirements of this section as it relates to the function of the individual security-sensitive employee and the training was provided within the schedule required for recurrent training; and

(2) Retains a record of such training in compliance with the requirements in paragraph (l).

(l) *Retention of security training records.* The owner/operator must retain records of initial and recurrent security training records for each individual required to receive security training under this section for no less than 5 years from the date of training that, at a minimum—

(1) Includes employee's full name, job title or function, date of hire, and date of initial and recurrent security training; and

(2) Identifies the date, course name, course length, and list of topics addressed for the security training most recently provided in each of the areas required under paragraph (f) of this section.

(m) *Availability of records to employees.* The owner/operator must provide records of security training to current and former employees upon request and at no charge as necessary to provide proof of training.

(n) *Incorporation into security program.* Once approved by TSA, the security training program required by this section is part of the owner/operator's TSA-approved

security program. The owner/operator must implement and maintain the security training program and comply with timeframes for implementation identified in the security training program. Any modifications or amendments to the program must be made as stipulated in § 1570.107 of this subchapter.

(o) *Situations requiring owner/operator to revise security training program.* The owner/operator must submit a request to amend its security program if, after approval, the owner/operator makes, or intends to make, permanent (to be in effect for 60 or more calendar days) or substantive changes to its security training curriculum, including changes to address:

(1) Determinations that the security training program is ineffective based on the approved method for evaluating effectiveness in the security training program approved by TSA; or

(2) Development of recurrent training material for purposes of meeting the requirements in paragraph (j) of this section or other alternative training materials not previously approved by TSA.

§ 1580.115 [Reserved]

17. Revise the heading of subpart C of part 1580 to read as follows:

Subpart C—Security of Rail Security-Sensitive Materials

18. Add subpart D of part 1580 to read as follows:

Subpart D—Cybersecurity Risk Management

Sec.
§ 1580.301 Scope and applicability.
§ 1580.303. Form, content, and availability of Cybersecurity Risk Management program.
§ 1580.305 Cybersecurity evaluation.
§ 1580.307 Cybersecurity Operational Implementation Plan.
§ 1580.309 Governance of the CRM program.
§ 1580.311 Cybersecurity Coordinator.
§ 1580.313 Identification of Critical Cyber Systems.
§ 1580.315 Supply chain risk management.
§ 1580.317 Protection of Critical Cyber Systems.
§ 1580.319 Cybersecurity training and knowledge.
§ 1580.321 Detection of cybersecurity incidents.

§ 1580.323 Capabilities to respond to a cybersecurity incident.
§ 1580.325 Reporting cybersecurity incidents.
§ 1580.327 Cybersecurity Incident Response Plan.
§ 1580.329 Cybersecurity Assessment Plan.
§ 1580.331 Documentation to establish compliance.

§ 1580.301 Scope and applicability.

(a) *Scope.* This subpart includes requirements to ensure the cybersecurity of freight rail operations and to mitigate the risk of significant harm to the individuals, cargo, and transportation facilities, as well as persons in areas in or near rail operations, that could have their safety and security threatened because of the degradation, destruction, or malfunction of systems that control these systems and infrastructure. In addition, cybersecurity incidents could have significant, similar impacts on the movement of cargo critical to the supply chain, affecting the national and economic security of the United States. The owner/operators identified in § 1580.1 must review the applicability for carrying out a Cybersecurity Risk Management program in paragraph (b) of this section, designation of a Cybersecurity Coordinator in § 1580.311, and reporting cybersecurity incidents in § 1580.325 to determine if the requirements apply to their operations.

(b) *Applicability.* Each owner/operator described in § 1580.1 must adopt and carry out a Cybersecurity Risk Management (CRM) program for any operation that meets any of the following criteria:

(1) Is a Class I freight railroad; or

(2) Is a Class II or III railroad, that:

(i) Provides switching or terminal services to two or more Class I railroads;

(ii) Transports one or more of the categories and quantities of RSSM in an HTUA;

(iii) Serves as a host railroad to a freight railroad described in paragraph (b)(1) or (b)(2) of this section or a passenger operation described in § 1582.201(b) of this

subchapter; or

(iv) Operates an average of at least 400,000 train miles in any of the three calendar years before [EFFECTIVE DATE OF FINAL RULE] or any single calendar year after [EFFECTIVE DATE OF FINAL RULE].

(3) Is designated as a Defense Connector Railroad.

§ 1580.303. Form, content, and availability of Cybersecurity Risk Management program.

(a) *General content requirements*. The CRM program required by this subpart is a comprehensive program that includes the following components:

(1) A cybersecurity evaluation completed and updated as required by § 1580.305;

(2) A TSA-approved Cybersecurity Operational Implementation Plan (COIP) that meets the requirements in § 1580.307.

(3) A Cybersecurity Assessment Plan that meets the requirements in § 1580.329.

(b) *Subsidiaries.* If a single CRM program is developed and implemented for multiple business units within a single corporate entity, any documents used to comply or establish compliance with the requirements in this subpart must clearly identify and distinguish application of the requirements to each business unit.

§ 1580.305 Cybersecurity evaluation.

(a) *General.* Each owner/operator required to have a CRM program must complete an initial and recurrent cybersecurity evaluation sufficient to determine the owner/operator's current enterprise-wide cybersecurity profile of logical/virtual and physical security controls when evaluated against the CRM program requirements in this subpart, using a form provided by TSA or other tools approved by TSA.

(b) *Timing.* The initial cybersecurity evaluation must be completed no later than [DATE 90 DAYS AFTER EFFECTIVE DATE OF FINAL RULE], but no more than one year before the date of submission of the owner/operator's Cybersecurity Operational

Implementation Plan required by § 1580.307. If commencing or modifying operations subject to these requirements after [EFFECTIVE DATE OF FINAL RULE], the initial cybersecurity evaluation must be submitted to TSA no later than 45 calendar days after commencing the new or modified operations triggering applicability.

(c) *Annual updates.* The evaluation required by paragraph (a) of this section must be updated annually, no later than one year from the anniversary date of the previously completed evaluation.

(d) *Notification.* The owner/operator must notify TSA within 7 days of completing the evaluation and annual updates required by this section. A copy of the evaluation must be provided to TSA upon request.

(e) *Sensitive Security Information.* This evaluation is a vulnerability assessment as defined in § 1500.3 of this subchapter and must be protected as Sensitive Security Information under § 1520.5(b)(5) of this subchapter.

§ 1580.307 Cybersecurity Operational Implementation Plan.

(a) *Requirement.* Each owner/operator required to have a CRM program under this part must adopt a COIP.

(b) *General Content.* The COIP must include the following corporate information:

(1) The name and corporate address of the owner/operator;

(2) Written attestation by the owner/operator's accountable executive that the COIP has been reviewed and approved by senior management; and

(3) Identification of specific operations that meet the applicability criteria.

(c) *Specific Content.* The COIP must detail the owner/operator's defense-in-depth plan, including physical and logical/virtual security controls, to comply with the requirements and security outcomes specified in the following sections:

(1) *Governance.* The requirements for governance of the CRM program in §

1580.309 and the designation of a Cybersecurity Coordinator in § 1580.311.

(2) *Identification of Critical Cyber Systems, Network Architecture, and Interdependencies.* The requirements to identify Critical Cyber Systems and network architecture in § 1580.313 and supply chain risk management in § 1580.315.

(3) *Procedures, policies, and capabilities to protect Critical Cyber Systems.* The requirements for protection of Critical Cyber Systems in § 1580.317 and training of cybersecurity-sensitive employees in § 1580.319.

(4) *Procedures, policies, and capabilities to detect cybersecurity incidents.* The requirements for detecting cybersecurity incidents in § 1580.321.

(5) *Procedures, policies, and capabilities to respond to, and recover from, cybersecurity incidents.* The requirements for responding to cybersecurity incidents in § 1580.323, reporting cybersecurity incidents in § 1580.325, and the Cybersecurity Incident Response Plan in § 1580.327.

(d) *Plan of Action and Milestones.* (1) To the extent an owner/operator does not meet every requirement and security outcome identified in paragraph (c)(1) through (c)(5) of this section, the COIP must include a plan of action and milestones (POAM).

(2) The POAM must include:

(i) Policies, procedures, measures, or capabilities that owner/operator will develop or obtain, as applicable, to ensure all requirements and security outcomes in this subpart are met;

(ii) Physical and logical/virtual security controls that the owner/operator will implement to mitigate the risks associated with not fully complying with requirements or security outcomes in this subpart; and

(iii) A detailed timeframe for full compliance with all requirements and security outcomes in this subpart, not to exceed 3 years from the date of submission to TSA of the COIP required by this section.

(3) The POAM must be updated as necessary to address any deficiencies identified during the evaluation required by § 1580.305 or as a result of an assessment conducted under § 1580.329 that will not be immediately addressed through an update to the COIP.

(e) *Approval and implementation.* (1) *Submission deadlines.* The COIP must be made available to TSA, in a form and manner prescribed by TSA, no later than [DATE 180 DAYS AFTER EFFECTIVE DATE OF FINAL RULE]. If commencing or modifying operations subject to these requirements after [EFFECTIVE DATE OF FINAL RULE], the COIP must be made available to TSA no later than 45 calendar days before commencing new or modified operations.

(2) *Effective date.* After considering all relevant materials and any additional information required by TSA, TSA will notify the owner/operator's accountable executive of TSA's decision to approve the owner/operator's COIP. The COIP becomes effective 30 days after the owner/operator is notified whether its COIP is approved.

(3) *TSA-approved security program.* Once approved by TSA, the COIP, any appendices, and any policies or procedures incorporated by reference, are a part of a TSA-approved security program, subject to the protections in part 1520 of this chapter and the procedures applicable to security programs in subpart B of part 1570 of this subchapter.

(f) *Status Report and Updates.* The CRM program must be reviewed and updated by the owner/operator within 60 days of the evaluations or assessments required by §§ 1580.305 or 1580.329, as necessary to address any identified vulnerabilities or weaknesses in the procedures, policies, or capabilities identified in the CRM program.

(g) *Revisions.* Unless otherwise specified in this subpart, any substantive modifications or amendments to the COIP must be made in accordance with the procedures in § 1570.107 of this subchapter.

§ 1580.309 Governance of the CRM program.

(a) *Accountable Executive.* (1) No later than [DATE 30 DAYS FROM EFFECTIVE DATE OF FINAL RULE], the owner/operator must provide to TSA the names, titles, business telephone numbers, and business email addresses of the owner/operator's accountable executive, who is the primary individual to be contacted with regard to the owner/operator's CRM program. If any of the information required by this paragraph changes, the owner/operator must provide the updated information to TSA within 7 days of the change.

(2) The accountable executive must be an individual who has the authority and knowledge necessary for the development, implementation, and managerial oversight of the TSA-approved CRM program, including cybersecurity administration, risk assessments, inspections and control procedures, and coordinating communications with the owner/operator's leadership and staff on implementation and sustainment of the CRM program. To the extent possible, the accountable executive should not be the Cybersecurity Coordinator or an individual responsible for management of Information or Operational Technology system or systems' administration.

(b) *COIP.* The COIP must also include:

(1) Identification of positions designated by the owner/operator to manage implementation of policies, procedures, and capabilities described in the COIP and coordinate improvements to the CRM program.

(2) Corporate-level identification of any authorized representatives, as defined in the TSA Cybersecurity Lexicon, who are responsible for any or all of the CRM program or cybersecurity measures identified in the CRM program, and written documentation (such as contractual agreements) clearly identifying the roles and responsibilities of the authorized representative under the CRM program.

(3) The information required by paragraph (a)(1) of this section.

(c) *Process.* Updating the COIP to align with information provided to TSA under this section does not require an amendment subject to the procedures in § 1570.107 of this subchapter.

§ 1580.311 Cybersecurity Coordinator.

(a)(1) Except as provided in paragraph (a)(2) of this section, each owner/operator identified in paragraphs § 1580.1(a)(1), (a)(4), and (a)(5) must designate employees at the corporate level to serve as the primary and at least one alternate Cybersecurity Coordinator with responsibility for sharing critical cybersecurity information.

(2) Each owner/operator identified in § 1580.1(a)(5) must designate and use a primary and at least one alternate Cybersecurity Coordinator, only if notified by TSA in writing that a threat exists concerning that type of operation.

(b) The Cybersecurity Coordinator and alternate(s) must—

(1) Serve as the primary contact for cyber-related intelligence information and cybersecurity-related activities and communications with TSA and the Cybersecurity and Infrastructure Security Agency (CISA);

(2) Have the following knowledge and skills, through current certifications or equivalent job experience:

(i) General cybersecurity guidance and best practices;

(ii) Relevant law and regulations pertaining to cybersecurity;

(iii) Handling of Sensitive Security Information and security-related communications; and

(iv) Current cybersecurity threats applicable to the owner/operator's operations and systems.

(3) Be accessible to TSA and CISA 24 hours per day, 7 days per week;

(4) Have a Homeland Security Information Network (HSIN) account or other TSA-designated communication platform for information sharing relevant to the

requirements in this subpart; and

(5) Work with appropriate law enforcement and emergency response agencies in addressing cybersecurity threats or responding to cybersecurity incidents.

(c) The Cybersecurity Coordinator and alternate(s) must be a U.S. citizen eligible for a security clearance, unless otherwise waived by TSA.

(d) Owner/operators must provide in writing to TSA the names, titles, business phone number(s), and business email address(es) of the Cybersecurity Coordinator and alternate Cybersecurity Coordinator(s) required by paragraph (a) of this section no later than [DATE 7 DAYS AFTER EFFECTIVE DATE OF FINAL RULE], or within 7 days of the commencement of new operations, or change in any of the information required by this section that occur after [DATE 7 DAYS AFTER EFFECTIVE DATE OF FINAL RULE].

(e) In addition to providing the information to TSA as required by paragraph (d), any owner/operator required to have a CRM program under this part must also include the information required by paragraph (d) in the COIP. As the owner/operator must separately notify TSA of this information, and any changes to this information, updating the COIP to align with information provided to TSA under this section does not require an amendment subject to the procedures in § 1570.107 of this subchapter.

§ 1580.313 Identification of Critical Cyber Systems.

(a) *Identifying information.* The owner/operator must incorporate into its COIP a list of Critical Cyber Systems, as defined in the TSA Cybersecurity Lexicon, that provides, at a minimum, the following identifying information for each Critical Cyber System:

(1) Identifier (system name or commercial name), and

(2) System manufacturer/designer name.

(b) *Identification methodology.* The owner/operator must include a description of

the methodology and information used to identify Critical Cyber Systems that, at a minimum, includes the following information as used to identify critical systems:

(1) Standards and factors, including system interdependencies with critical functions, used to identify Information Technology and Operational Technology systems that could be vulnerable to a cybersecurity incident;

(2) Sources and data, such as known threat information relevant to the system, that informed decisions regarding the likelihood of the system being subject to a cybersecurity incident;

(3) Potential operational impacts of a cybersecurity incident, including scenarios that identify potential supply chain impacts and how long critical operations and capabilities could be sustained with identified alternatives if a system is offline; and

(4) Sustainability and operational impacts if an Information or Operational Technology system not identified as a Critical Cyber System becomes unavailable due to a cybersecurity incident.

(c) *Positive Train Control (PTC) Systems.* Owner/operators who are either required to install and operate PTC under 49 CFR part 236, subpart I, and/or voluntarily install and operate PTC under CFR part 236, subpart H or I, must include PTC systems as a Critical Cyber System.

(d) *System information and network architecture.* For all Critical Cyber Systems, the owner/operator must provide the following information:

(1) Information and Operational Technology system interdependencies for Critical Cyber Systems;

(2) All external connections to Critical Cyber Systems;

(3) Zone boundaries for Critical Cyber Systems, including a description of how Information and Operational Technology systems are defined and organized into logical/virtual zones based on criticality, consequence, and operational necessity;

(4) Baseline of acceptable communications between Critical Cyber Systems and external connections or between Information and Operational Technology systems; and

(5) Operational needs that prevent or delay implementation of the requirements in this subpart, such as application of security patches and updates, encryption of communications traversing Information and Operational Technology systems, and multi-factor authentication.

(e) *Additional systems.* If notified by TSA, the owner/operator must include additional Critical Cyber Systems identified by TSA not previously identified by the owner/operator.

(f) *Changes in Critical Cyber Systems.* Any substantive changes to Critical Cyber Systems require an amendment to the COIP subject to the procedures in § 1570.107 of this subchapter.

§ 1580.315 Supply chain risk management.

The owner/operator must incorporate into its COIP policies, procedures, and capabilities to address supply chain cybersecurity vulnerabilities that include requiring—

(a) All procurement documents and contracts, including service-level agreements, executed or updated after [EFFECTIVE DATE OF FINAL RULE] include a requirement for the vendor or service provider to notify the owner/operator of the following:

(1) Cybersecurity incidents affecting the vendor or service provider within a specified timeframe sufficient for the owner/operator to identify and address any potential risks to their Critical Cyber Systems based on the scope and type of cybersecurity incident.

(2) Confirmed security vulnerabilities affecting the goods, services, or capabilities provided by the vendor or service provider within a specified timeframe sufficient for the owner/operator to identify and address any potential risks to their Critical Cyber Systems based on the scope and type of security vulnerability.

(b) Procurement documents and contracts, including service-level agreements, incorporate an evaluation by the owner/operator or qualified third-party of the cybersecurity measures implemented by vendors or service providers of goods, services, or capabilities that will be connected to, installed on, or used by the owner/operator's Critical Cyber Systems.

(c) When provided two offerings of roughly similar cost and function, giving preference to the offering that provides the greater level of cybersecurity necessary to protect against, or effectively respond to, cybersecurity incidents affecting the owner/operator's Critical Cyber Systems.

(d) Upon notification of a cybersecurity incident or vulnerability under paragraphs (a) or (b) of this section, immediate consideration of mitigation measures sufficient to address the resulting risk to Critical Cyber Systems and, as applicable, revision to the COIP in accordance with § 1570.107 of this subchapter.

§ 1580.317 Protection of Critical Cyber Systems.

The owner/operator must incorporate into its COIP policies, procedures, controls and capabilities to protect Critical Cyber Systems that meet security performance objectives in the following areas—

(a) *Network segmentation.* Network segmentation measures that protect against access to, or disruption of, the Operational Technology system if the Information Technology system is compromised or vice versa. These measures must be sufficient to—

(1) Ensure Information and Operational Technology system-services transit the other only when necessary for validated business or operational purposes;

(2) Secure and defend zone boundaries with security controls—

(i) To defend against unauthorized communications between zones; and

(ii) To prohibit Operational Technology system services from traversing the

Information Technology system, and vice-versa, unless the content is encrypted at a level sufficient to secure and protect integrity of data and prevent corruption or compromise while in transit. If encryption is not technologically feasible, ensure content is otherwise secured and protected using compensating controls that provide the same level of security as encryption for data in transit.

(b) *Access control.* Access control measures for Critical Cyber Systems, including for local and remote access, that secure and defend against unauthorized access to Critical Cyber Systems. Except as provided in paragraph (f), these measures must, at a minimum, incorporate the following policies, procedures, and controls:

(1) Identification and authentication requirements designed to prevent unauthorized access to Critical Cyber Systems, to include:

(i) A policy for memorized secret authenticator resets that includes criteria for passwords and when resets must occur, including procedures to ensure implementation of these requirements, such as password lockouts; and

(ii) Documented and defined logical/virtual and physical security controls for components of Critical Cyber Systems that will not be subject to the requirements in paragraph (b)(1)(i) of this section.

(2) Multi-factor authentication, or other logical/virtual and physical security controls to supplement memorized secret authenticators (such as passwords) to provide risk mitigation commensurate to multi-factor authentication. If an owner/operator does not apply multi-factor authentication for access to Operational Technology components or assets, the owner/operator must specify what compensating controls are used to manage access.

(3) Management of access rights based on the principles of least privilege and separation of duties. Where not technically feasible to apply these principles, the policies and procedures must describe compensating controls that the owner/operator applies.

(4) Policies and procedures limit availability and use of shared accounts to those that are critical for operations, and then only if absolutely necessary. When the owner/operator uses shared accounts for operational purposes, the policies and procedures must ensure:

(i) Access to shared accounts is limited through account management that uses principles of least privilege and separation of duties;

(ii) Any individual who no longer needs access does not have knowledge of the memorized secret authenticator necessary to access the shared account; and

(iii) Logs are maintained sufficient to enable positive user identification of access to shared accounts to enable forensic investigation following a cybersecurity incident.

(5) Regularly updated schedule for review of existing domain trust relationships to ensure their necessity and established and enforced policies to manage these relationships.

(c) *Patch management.* Measures that reduce the risk of exploitation of unpatched systems through the application of security patches and updates for operating systems, applications, drivers, and firmware on Critical Cyber Systems consistent with the owner/operator's risk-based methodology. These measures must include:

(1) A patch management strategy that ensures all critical security patches and updates on Critical Cyber Systems are current. This strategy must include:

(i) The risk methodology for categorizing and determining criticality of patches and updates, and an implementation timeline based on categorization and criticality; and

(ii) Prioritization of all security patches and updates on CISA's Known Exploited Vulnerabilities Catalog.

(2) In instances where the owner/operator cannot apply patches and updates on specific Operational Technology systems without causing a severe degradation of operational capability to meet business critical functions, the owner/operator must

provide an explanation for why the actions cannot be taken and a description and timeline of additional mitigations that address the risk created by not installing the patch or update within the recommended timeframe.

(d) *Logging policies.* Logging policies sufficient to ensure logging data is—

(1) Stored in a secure and centralized system, such as a security information and event management tool or database on a segmented network that can only be accessed or modified by authorized and authenticated users; and

(2) Maintained for a duration sufficient to allow for investigation of cybersecurity incidents as supported by a risk analysis and applicable standards or regulatory guidelines.

(e) *Secure back-ups.* Policies that ensure all Critical Cyber Systems are backed-up on a regular basis consistent with operational need for the information, the back-ups are securely stored separate from the system, and policies that require testing the integrity of back-ups to ensure that the data is free of known malicious code when the back-ups are made.

(f) *Exception for PTC hardware and software components installed on locomotive.* (1) For hardware and software components of a PTC system installed on a locomotive, owner/operators in compliance with requirements in 49 CFR 232.105(h)(1-4) (General requirements for locomotives), 49 CFR 236.3 (Locking of signal apparatus housings), and 49 CFR 256.553 (Seal, where required), may rely on the physical security measures used to comply with these requirements, as applicable, in lieu of implementing the requirements in paragraph (b).

(2) If relying on the exception in paragraph (f)(1), the owner/operator must list the applicable PTC system as a Critical Cyber System; maintain compliance with the requirements specified in 49 CFR 232.105(h)(1-4), 49 CFR 236.3, and 49 CFR 256.553, as applicable; and include in the COIP a description of the physical security measures

used to prevent unauthorized access to the identified PTC components.

§ 1580.319 Cybersecurity training and knowledge.

(a) *Training required.* (1) Owner/operators required to have a CRM program under this subchapter must provide basic cybersecurity training to all employees, with access to the owner/operator's Information or Operational Technology systems.

(2) No owner/operator required to have a CRM program under this subpart may permit a cybersecurity-sensitive employee to access, or have privileges to access, a Critical Cyber System or an Information or Operational Technology system that is interdependent with a Critical Cyber System, unless that individual has received basic and role-based cybersecurity training.

(b) *General curriculum requirements.* The cybersecurity training program must include a curriculum or lesson plan, including learning objectives and method of delivery (such as instructor-led or computer-based training) for each course used to meet the requirements in paragraphs (d) and (e) of this section. TSA may request additional information regarding the curriculum during the review and approval process. If recurrent training under paragraph (e) of this section is not the same as initial training, a curriculum or lesson plan for the recurrent training will need to be submitted and approved by TSA.

(c) *Specific curriculum requirements.* (1) *Basic cybersecurity training.* All employees and contractors with access to the owner/operator's Information or Operational Technology systems, must receive basic cybersecurity training that includes cybersecurity awareness to address best practices, acceptable use, risks associated with their level of privileged access, and awareness of security risks associated with their actions. This training must address the following topics:

(i) Social engineering, including phishing;

(ii) Password best practices;

(iii) Remote work security basics;

(iv) Safe internet and social media use;

(v) Mobile device (wireless) vulnerabilities and network security;

(vi) Data management and information security, including protecting business email, confidential information, trade secrets, and privacy; and

(vii) How and to whom to report suspected inappropriate or suspicious activity involving Information or Operational Technology systems, including mobile devices provided by or connected to the owner/operator's Information or Operational Technology systems.

(2) *Role-based cybersecurity training.* Cybersecurity-sensitive employees must be provided cybersecurity training that specifically addresses their role as a privileged user to prevent and respond to a cybersecurity incident, acceptable uses, and the risks associated with their level of access and use as approved by the owner/operator. This training must address the following topics as applicable to the specific role:

(i) Security measures and requirements in the COIP including how the requirements affect account and access management, server and application management, and system architecture development and assessment;

(ii) Recognition and detection of cybersecurity threats, types of cybersecurity incidents, and techniques used to circumvent cybersecurity measures;

(iii) Incident handling, including procedures for reporting a cybersecurity incident to the Cybersecurity Coordinator and understanding their roles and responsibilities during a cybersecurity incident and implementation of the owner/operator's Cybersecurity Incident Response Plan required by § 1580.327;

(iv) Requirements and sources for staying aware of changing cybersecurity threats and countermeasures; and

(v) Operational Technology-specific cybersecurity training for all personnel

whose duties include access to Operational Technology systems.

(d) *Initial cybersecurity training.* (1) Each owner/operator must provide initial cybersecurity training (basic and role-based, as applicable) to employees and contractors, using the curriculum approved by TSA no later than 60 days after the effective date of the owner/operator's TSA-approved COIP required by this subpart.

(2) For individuals who onboard or become cybersecurity-sensitive employees after the effective date of the owner/operator's TSA-approved COIP who did not receive training within the period identified in paragraph (d)(1) of this section, the individual must receive the applicable cybersecurity training no later than 10 days after onboarding.

(e) *Recurrent cybersecurity training.* Employees and contractors must receive annual recurrent cybersecurity training no later than the anniversary calendar month of the employee's initial cybersecurity training. If the owner/operator provides the recurrent cybersecurity training in the month of, the month before, or the month after it is due, the employee is considered to have taken the training in the month it is due.

(f) *Recognition of prior or established cybersecurity training.* Previously provided cybersecurity training may be credited towards satisfying the requirements of this section provided the owner/operator—

(1) Obtains a complete record of such training and validates the training meets requirements of this section as it relates to the role of the individual employee, and the training was provided within the schedule required for recurrent training; and

(2) Retains a record of such training in compliance with the requirements in paragraph (g) of this section.

(g) *Retention of cybersecurity training records.* The owner/operator must retain records of initial and recurrent cybersecurity training records for each individual required to receive cybersecurity training under this section for no less than 5 years from the date of training that, at a minimum—

(1) Includes the employee's full name, job title or function, date of hire, and date of initial and recurrent cybersecurity training; and

(2) Identifies the date, course name, course length, and list of topics addressed for the cybersecurity training most recently provided in each of the areas required under paragraph (c) of this section.

(h) *Availability of records to employees.* The owner/operator must provide records of cybersecurity training to current and former employees upon request and at no charge as necessary to provide proof of training.

§ 1580.321 Detection of cybersecurity incidents.

The owner/operator must incorporate into its COIP policies, procedures, and capabilities sufficient to detect and respond to cybersecurity threats to, and anomalies on, Critical Cyber Systems that, at a minimum—

(a) Defend against malicious email, such as spam and phishing emails, to preclude or mitigate against adverse impacts to operations;

(b) Block ingress and egress communications with known or suspected malicious Internet Protocol addresses;

(c) Control impact of known or suspected malicious web domains or web applications, such as by preventing users and devices from accessing malicious websites;

(d) Block and defend against unauthorized code, including macro scripts, from executing;

(e) Monitor and/or block connections from known or suspected malicious command and control servers (such as Tor exit nodes, and other anonymization services); and

(f) Ensure continuous collection and analysis of data for potential intrusions and anomalous behavior on Critical Cyber Systems and other Information and Operational Technology systems that directly connect with Critical Cyber Systems.

§ 1580.323 Capabilities to respond to a cybersecurity incident.

The owner/operator must incorporate into its COIP capabilities to respond to cybersecurity incidents affecting Critical Cyber Systems that, at a minimum—

(a) Audit unauthorized access to internet domains and addresses;

(b) Document and audit any communications between the Operational Technology system and an internal or external system that deviates from the owner/operator's identified baseline of communications;

(c) Identify and respond to execution of unauthorized code, including macro scripts; and

(d) Define, prioritize, and drive standardized incident response activities, such as Security Orchestration, Automation, and Response (SOAR).

§ 1580.325 Reporting cybersecurity incidents.

(a) Unless otherwise directed by TSA, each owner/operator identified in § 1580.1(a)(1), (a)(4), and (a)(5) must notify CISA of any Reportable Cybersecurity Incidents, as defined in the TSA Cybersecurity Lexicon, as soon as practicable, but no later than 24 hours after a Reportable Cybersecurity Incident is identified.

(b) Reports required by this section must be made by the methods prescribed by TSA. All reported information will be protected in a manner appropriate for the sensitivity and criticality of the information.

(c) The report to CISA must include the following information, as available to the reporting owner/operator at the time of the report:

(1) The name of the reporting individual and contact information, including a telephone number and email address. The report must also explicitly specify that the information is being reported in order to satisfy the reporting requirements in Transportation Security Regulations.

(2) The affected rail system(s) or facilities, including identifying information and

location.

(3) Description of the threat, incident, or activity, to include:

(i) Earliest known date of compromise;

(ii) Date of detection;

(iii) Information about who has been notified and what action has been taken;

(iv) Any relevant information observed or collected by the owner/operators, such as malicious Internet Protocol addresses, malicious domains, malware hashes and/or samples, or the abuse of legitimate software or accounts; and

(v) Any known threat information, to include information about the source of the threat or cybersecurity incident, if available.

(4) A description of the incident's impact or potential impact on Information or Operational Technology systems and operations. This information must also include an assessment of actual or imminent adverse impacts to service operations, operational delays, and/or data theft that have or are likely to be incurred, as well as any other information that would be informative in understanding the impact or potential impact of the cybersecurity incident.

(5) A description of all responses that are planned or under consideration, to include, for example, a reversion to manual operations of train movement and control, if applicable.

(6) Any additional information not specifically required by this section, but which is critical to an understanding of the threat and owner/operator's response to a reportable cybersecurity incident.

(d) If all the required information is not available at the time of reporting, owner/operators must submit an initial report within the specified timeframe and supplement as additional information becomes available.

§ 1580.327 Cybersecurity Incident Response Plan.

(a) The owner/operator must incorporate into its COIP an up-to-date Cybersecurity Incident Response Plan (CIRP) for the owner/operator's Critical Cyber Systems to reduce the impacts of a cybersecurity incident that causes, or could cause, operational disruption or significant impacts on business-critical functions.

(b) The CIRP must provide specific measures sufficient to ensure the following objectives, as applicable:

(1) Promptly identifying, isolating, and segregating the infected systems from uninfected systems, networks, and devices using measures that prioritize:

(i) Limiting the spread of autonomous malware;

(ii) Denying continued access by a threat actor to systems;

(iii) Determining extent of compromise; and

(iv) Preserving evidence and data.

(2) Only data stored and secured as required by § 1580.317(e) is used to restore systems and that all stored backup data is scanned with host security software to ensure the data is free of malicious artifacts before being used for restoration.

(3) Established capability and governance for implementing mitigation measures or manual controls that ensure that the Operational Technology system can be isolated when a cybersecurity incident in the Information Technology system creates risk to the safety and reliability of the Operational Technology system.

(c) The CIRP must identify who (by position) is responsible for implementing the specific measures in the plan and any necessary resources needed to implement the measures.

(d) The owner/operator must conduct an exercise to test the effectiveness of the CIRP no less than annually. The exercise conducted under this paragraph must—

(1) Test at least two objectives of the owner/operator's CIRP required by paragraph (b) of this section, no less than annually; and

(2) Include the employees identified (by position) in paragraph (c) as active participants in the exercise.

(e) Within no more than 90 days after the date of the exercise required by paragraph (d), the owner/operator must update the CIRP as appropriate to address any issues identified during the exercise.

(f) The owner/operator must notify TSA within 15 days of any changes to the CIRP. As the owner/operator must separately notify TSA, updating the COIP to align with information provided to TSA under this section does not require an amendment subject to the procedures in § 1570.107 of this subchapter.

§ 1580.329 Cybersecurity Assessment Plan.

(a) *Requirement for a Cybersecurity Assessment Plan.* No later than 90 days from TSA's approval of the owner/operator's COIP, the owner/operator must submit to TSA a Cybersecurity Assessment Plan (CAP) sufficient to—

(1) Proactively assess the effectiveness of all policies, procedures, measures, and capabilities in the owner/operator's TSA-approved COIP as applied to all Critical Cyber Systems; and

(2) Identify and resolve device, network, and/or system vulnerabilities associated with Critical Cyber Systems.

(b) *Contents of the CAP.* At a minimum, the CAP must describe in detail:

(1) The plan to assess the effectiveness of the owner/operator's TSA-approved COIP and applied to all Critical Cyber Systems;

(2) Schedule and scope of an architectural design review within 12 months either before or after TSA's approval of the owner/operator's COIP, to be repeated at least once every 2 years thereafter. The architectural design review required by this paragraph must include verification and validation of network traffic, a system log review, and analysis to identify cybersecurity vulnerabilities related to network design, configuration, and

interconnectivity to internal and external systems;

(3) Other assessment capabilities designed to identify vulnerabilities to Critical Cyber Systems based on evolving threat information and adversarial capabilities, such as penetration testing of Information Technology systems, including the use of "red" and "purple" team (adversarial perspective) testing.

(c) *Specific Schedule.* (1) In addition to specifying the schedule for the architectural design review required by paragraph (b)(2), the CAP must include a schedule for conducting the assessments required by paragraph (b) sufficient to ensure at least one-third of the policies, procedures, measures, and capabilities in the TSA-approved COIP are assessed each year, with 100 percent of the COIP and all Critical Cyber Systems assessed over a 3-year period.

(2) The schedule required by this paragraph must map the planned assessments to the COIP and Critical Cyber System to document the plan will ensure all policies, procedures, measures, and capabilities in the owner/operator's TSA-approved COIP and all Critical Cyber Systems will be assessed within the timeframes required by paragraph (c)(1).

(d) *Independence of assessors and auditors.* Owner/operators must ensure that the assessments, audits, testing, and other capabilities to assess the effectiveness of its TSA-approved COIP are not conducted by individuals who have oversight or responsibility for implementing the owner/operator's CRM program and have no vested or other financial interest in the results of the CAP.

(e) *Annual submission of report.* The owner/operator must ensure a report of the results of assessments conducted in accordance with the CAP is provided to corporate leadership and individuals designated under § 1580.309(a) and (b)(1) of this subpart, and submitted to TSA, no later than 15 months from the date of approval of the initial CAP and annually thereafter. The required report must indicate—

(1) Which assessment method(s) were used to determine if the policies, procedures, and capabilities described by the owner/operator in its COIP are effective; and

(2) Results of the assessment methodologies.

(f) *Annual update of the CAP.* The owner/operator must review and annually update the CAP to address any changes to policies, procedures, measures, or capabilities in the COIP or assessment capabilities required by paragraph (b). The updated CAP must be submitted to TSA for approval no later than 12 months from the date of TSA's approval of the current CAP.

(g) *Sensitive Security Information.* Assessments conducted under this section are vulnerability assessments as defined in § 1500.3 of this chapter and must be protected as Sensitive Security Information under § 1520.5(b)(5) of this chapter.

§ 1580.331 Documentation to establish compliance.

For the purposes of the requirements in this subpart, upon TSA's request, the owner/operator must provide for inspection or copying the following types of information to establish compliance:

(a) Hardware/software asset inventory, including supervisory control and data acquisition (SCADA) systems;

(b) Firewall rules;

(c) Network diagrams, switch and router configurations, architecture diagrams, publicly routable internet protocol addresses, and Virtual Local Area Networks;

(d) Policy, procedural, and other documents that informed the development, and documented implementation of, the owner/operator's CRM program;

(e) Data providing a "snapshot" of activity on and between Information and Operational Technology systems such as:

(1) Log files;

(2) A capture of network traffic (such as packet capture (PCAP)), for a scope and period directed by TSA, not less than 24 hours and not to exceed 48 hours;

(3) "East-West Traffic" of Information Technology systems, sites, and environments within the scope of this subpart; and

(4) "North-South Traffic" between Information and Operational Technology systems, and the perimeter boundaries between them; and

(f) Any other records or documents necessary to determine compliance with this subpart.

19. Revise appendix B to part 1580 to read as follows:

Appendix B to Part 1580—Security-Sensitive Functions for Freight Rail

This table identifies security-sensitive job functions for owner/operators regulated under this part. All employees performing security-sensitive functions are "security-sensitive employees" for purposes of this rule and must be trained in accordance with this part.

Categories	Security-Sensitive Job Functions for Freight Rail	Examples of Job Titles Applicable to These Functions*
A. Operating a vehicle ….	1. Employees who operate or directly control the movements of locomotives or other self-powered rail vehicles. 2. Train conductor, trainman, brakeman, or utility employee or performs acceptance inspections, couples and uncouples rail cars, applies handbrakes, or similar functions. 3. Employees covered under the Federal hours of service laws as "train employees." *See* 49 U.S.C. 21101(5) and 21103.	Engineer, conductor
B. Inspecting and maintaining vehicles ..	Employees who inspect or repair rail cars and locomotives.	Carman, car repairman, car inspector, engineer, conductor
C. Inspecting or maintaining building or transportation infrastructure …..	1. Employees who— a. Maintain, install, or inspect communications and signal equipment. b. Maintain, install, or inspect track and structures, including, but not limited to, bridges, trestles, and tunnels. 2. Employees covered under the Federal hours of service laws as "signal employees." *See* 49 U.S.C. 21101(3) and 21104.	Signalman, signal maintainer, trackman, gang foreman, bridge and building laborer, roadmaster, bridge, and building inspector/operator

D. Controlling dispatch or movement of a vehicle …….	1. Employees who— a. Dispatch, direct, or control the movement of trains. b. Operate or supervise the operations of moveable bridges. c. Supervise the activities of train crews, car movements, and switching operations in a yard or terminal. 2. Employees covered under the Federal hours of service laws as "dispatching service employees." *See* 49 U.S.C. 21101(2) and 21105.	Yardmaster, dispatcher, block operator, bridge operator
E. Providing security of the owner / operator's equipment and property ……..……...	Employees who provide for the security of the railroad carrier's equipment and property, including acting as a railroad police officer (as that term is defined in 49 CFR 207.2).	Police officer, special agent; patrolman; watchman; guard
F. Loading or unloading cargo or baggage ..…	Includes, but is not limited to, employees that load or unload hazardous materials.	Service track employee
G. Interacting with travelling public (on board a vehicle or within a transportation facility) …….	Employees of a freight railroad operating in passenger service.	Conductor, engineer, agent
H. Complying with security programs or measures, including those required by Federal law …….....	1. Employees who serve as security coordinators designated in §§ 1580.103 or 1580.311 of this subchapter, as well as any designated alternates or secondary security coordinators. 2. Employees who— a. Conduct training and testing of employees when the training or testing is required by TSA's security regulations. b. Perform inspections or operations required by § 1580.205 of this subchapter. c. Manage or direct implementation of security plan requirements.	Security coordinator, accountable executive train master, assistant train master, roadmaster, division roadmaster

* These job titles are provided solely as a resource to help understand the functions described; whether an employee must be trained is based upon the function, not the job title.

20. Add appendix C to part 1580 to read as follows:

Appendix C to Part 1580—Reporting of Significant Physical Security Concerns

Category	Description
Breach, Attempted Intrusion, and/or Interference ……..…	Unauthorized personnel attempting to or actually entering a restricted area or secure site relating to a transportation facility or conveyance owned, operated, or used by an owner/operator subject to this part. This includes individuals entering or attempting to enter by impersonation of authorized personnel (for example, police/security, janitor, vehicle owner/operator). Activity that could interfere with the ability of employees to perform duties to the extent that security is threatened.
Misrepresentation ……..……	Presenting false, or misusing, insignia, documents, and/or identification, to misrepresent one's affiliation with an owner/operator subject to this part to cover possible illicit activity that may pose a risk to transportation security.
Theft, Loss, and/or Diversion	Stealing or diverting identification media or badges, uniforms, vehicles, keys, tools capable of compromising track integrity, portable derails, technology, or classified or sensitive security information documents which are proprietary to the facility or conveyance owned, operated, or used by an owner/operator subject to this part.

Category	Description
Sabotage, Tampering, and/or Vandalism ……..	Damaging, manipulating, or defeating safety and security appliances in connection with a facility, infrastructure, conveyance, or routing mechanism, resulting in the compromised use or the temporary or permanent loss of use of the facility, infrastructure, conveyance or routing mechanism. Placing or attaching a foreign object to a rail car(s).
Expressed or Implied Threat …….....	Communicating a spoken or written threat to damage or compromise a facility/infrastructure/conveyance owned, operated, or used by an owner/operator subject to this part (for example, a bomb threat or active shooter).
Eliciting Information ……	Questioning that may pose a risk to transportation or national security, such as asking one or more employees of an owner/operator subject to this part about particular facets of a facility's conveyance's purpose, operations, or security procedures.
Testing or Probing of Security……	Deliberate interactions with employees of an owner/operator subject to this part or challenges to facilities or systems owned, operated, or used by an owner/operator subject to this part that reveal physical, personnel, or security capabilities or sensitive information.
Photography ……	Taking photographs or video of facilities, conveyances, or infrastructure owned, operated, or used by an owner/operator subject to this part in a manner that may pose a risk to transportation or national security. Examples include taking photographs or video of infrequently used access points, personnel performing security functions (for example, patrols, badge/vehicle checking), or security-related equipment (for example, perimeter fencing, security cameras).
Observation or Surveillance	Demonstrating unusual interest in facilities or loitering near conveyances, railcar routing appliances or any potentially critical infrastructure owned or operated by an owner/operator subject to this part in a manner that may pose a risk to transportation or national security. Examples include observation through binoculars, taking notes, or attempting to measure distances.
Materials Acquisition and/or Storage ……	Acquisition and/or storage by an employee of an owner/operator subject to this part of materials such as cell phones, pagers, fuel, chemicals, toxic materials, and/or timers that may pose a risk to transportation or national security (for example, storage of chemicals not needed by an employee for the performance of his or her job duties).
Weapons Discovery, Discharge, or Seizure…….	Weapons or explosives in or around a facility, conveyance, or infrastructure of an owner/operator subject to this part that may present a risk to transportation or national security (for example, discovery of weapons inconsistent with the type or quantity traditionally used by company security personnel).
Suspicious Items or Activity ..	Discovery or observation of suspicious items, activity or behavior in or around a facility, conveyance, or infrastructure of an owner/operator subject to this part that results in the disruption or termination of operations (for example, halting the operation of a conveyance while law enforcement personnel investigate a suspicious bag, briefcase, or package).

PART 1582—PUBLIC TRANSPORTATION AND PASSENGER RAILROAD SECURITY

21. Revise the authority citation for part 1582 to read as follows:

Authority: 49 U.S.C. 114; Pub. L. 110-53, 121 Stat. 266.

22. Amend § 1582.3 by adding the definition of "Unlinked passenger trips" in alphabetical order.

§ 1582.3 Terms used in this part.

* * * * *

Unlinked passenger trips means the number of times passengers board public transportation vehicles based on counting passengers each time they board vehicles, no matter how many vehicles they use to travel from their origin to their destination and regardless of whether they pay a fare, use a pass or transfer, ride for free, or pay in some other way.

23. Revise subpart B of part 1582 to read as follows:

Subpart B—Security Programs: Physical Security

Sec.
§ 1582.101 Scope.
§ 1582.103 Physical Security Coordinator.
§ 1582.105 Reporting of significant physical security concerns.
§ 1582.107 [Reserved]
§ 1582.109 [Reserved]
§ 1582.111 [Reserved]
§ 1582.113 Security training program requirements.
§ 1582.115 [Reserved]

§ 1582.101 Scope.

This subpart includes requirements that are primarily intended to ensure the physical security of public transportation and passenger railroads. Physical security encompasses the security of individuals, buses, rail cars, and transportation facilities, as well as the persons in areas in or near to operations that could have their safety and security threatened by an attack on physical systems and assets. Owner/operators identified in § 1582.1 must review the applicability in each section in this subpart to determine if any of the requirements apply to their operations.

§ 1582.103 Physical Security Coordinator.

(a) (1) Except as provided in (a)(2) and (3) of this paragraph, each owner/operator identified in § 1582.1 must designate and use a primary and at least one alternate Physical Security Coordinator at the corporate level to function as the administrator for sharing security-related activities and information.

(2) An owner/operator identified in § 1582.1(a)(2) that owns or operates a bus-

only operation must designate and use a primary and at least one alternate Physical Security Coordinator only if the owner/operator is identified in appendix A to part 1582 of this subchapter or is notified by TSA in writing that a threat exists concerning that operation.

(3) An owner/operator identified in § 1582.1(a)(4) (tourist, scenic, historic, or excursion rail operations) must designate and use a primary and at least one alternate Physical Security Coordinator, only if notified by TSA in writing that a threat exists concerning that type of operation.

(b) The primary Physical Security Coordinator and alternate(s) must—

(1) Be accessible to TSA on a 24 hours per day, 7 days per week basis; and

(2) Serve as the primary contact(s) for intelligence information and security-related activities and communications with TSA. Any individual designated as a Physical Security Coordinator may perform other duties in addition to the duties described in this section); and

(3) Coordinate security practices and procedures required by this subchapter internally and with appropriate law enforcement and emergency response agencies.

(c) The Physical Security Coordinator and alternate(s) must be a U.S. citizen eligible for a security clearance, unless otherwise waived by TSA.

(d) Each owner/operator required to have a Physical Security Coordinator must provide in writing to TSA the names, U.S. citizenship status, titles, business phone number(s), and business email address(es) of the Physical Security Coordinator and alternate(s). Changes in any of the information required by this section must be submitted to TSA within 7 calendar days.

§ 1582.105 Reporting of significant physical security concerns.

(a) Each owner/operator identified in § 1582.1 must report, within 24 hours of initial discovery, any potential threats and significant physical security concerns

involving transportation-related operations in the United States or transportation to, from, or within the United States as soon as possible by the methods prescribed by TSA.

(b) Potential threats or significant physical security concerns encompass incidents, suspicious activities, and threat information affecting physical operations including, but not limited to, the categories of reportable events listed in appendix C to this part.

(c) Information reported must include the following, as available and applicable:

(1) The name of the reporting individual and contact information, including a telephone number or email address.

(2) The affected freight or passenger train, bus, conveyance, station, terminal, rail hazardous materials facility, or other transportation facility or infrastructure, including identifying information and current location.

(3) Scheduled origination and termination locations for the affected passenger train or bus –including departure and destination station, city, and route, as applicable.

(4) Description of the threat, incident, or activity, including who has been notified and what action has been taken.

(5) The names, other available biographical data, and/or descriptions (including vehicle or license plate information) of individuals or motor vehicles known or suspected to be involved in the threat, incident, or activity.

(6) The source of any threat information.

§ 1582.107 [Reserved]

§ 1582.109 [Reserved]

§ 1582.111 [Reserved]

§ 1582.113 Security training program requirements.

(a) *Applicability.* This section applies to the following:

(1) Amtrak (also known as the National Railroad Passenger Corporation).

(2) Each owner/operator identified in Appendix A to this part.

(3) Each owner/operator described in § 1582.1(a)(1) through (3) that serves as a host railroad to a freight operation described in § 1580.113(a) of this subchapter or to a passenger train operation described in paragraphs (1) or (2) of this section.

(b) *Training required for security-sensitive employees.* No owner/operator identified in paragraph (a) of this section may use a security-sensitive employee to perform a function identified in Appendix B to this part, unless that individual has received training as part of a security training program approved by TSA or is under the direct supervision of an employee who has received the training required by this section as applicable to that security-sensitive function. Upon approval, this security training program becomes part of the owner/operators TSA-approved security program.

(c) *Limits on use of untrained employees.* Notwithstanding paragraph (b) of this section, a security-sensitive employee may not perform a security-sensitive function for more than 60 calendar days without receiving security training.

(d) *General requirements.* Each owner/operator required to provide security training to its employees under this section must submit their security training program to TSA for approval in a form and manner prescribed by TSA. The security training program must include the following information:

(1) Name of owner/operator.

(2) Name, title, telephone number, and email address of the primary individual to be contacted with regard to review of the security training program.

(3) Number, by specific job function category identified in Appendix B to this part, of security-sensitive employees trained or to be trained.

(4) Implementation schedule that identifies a specific date by which the required initial and recurrent security training will be completed.

(5) Location where training program records will be maintained.

(6) Plan for ensuring supervision of untrained security-sensitive employees

performing functions identified in Appendix B to this part.

(7) Plan for notifying employees of changes to security measures that could change information provided in previously provided training.

(8) Method(s) for evaluating the effectiveness of the security training program in each area required by paragraph (e) of this section.

(e) *General curriculum requirements.* The security training program submitted to TSA for approval must include a curriculum or lesson plan, including learning objectives and method of delivery (such as instructor-led or computer-based training) for each course used to meet the requirements in paragraph (f) of this section. TSA may request additional information regarding the curriculum during the review and approval process. If recurrent training under paragraph (j) of this section is not the same as initial training, a curriculum or lesson plan for the recurrent training will need to be submitted and approved by TSA.

(f) *Specific curriculum requirements.* (1) *Prepare.* Each owner/operator must ensure that each of its security-sensitive employees with position- or function-specific responsibilities under the owner/operator's security program have knowledge of how to fulfill those responsibilities in the event of a security threat, breach, or incident to ensure—

(i) Employees with responsibility for transportation security equipment and systems are aware of their responsibilities and can verify the equipment and systems are operating and properly maintained; and

(ii) Employees with other duties and responsibilities under the company's security plans and/or programs, including those required by Federal law, know their assignments and the steps or resources needed to fulfill them.

(2) *Observe.* Each owner/operator must ensure that each of its security-sensitive employees has knowledge of the observational skills necessary to recognize—

(i) Suspicious and/or dangerous items, such as substances, packages, or conditions (for example, characteristics of an Improvised Explosive Device and signs of equipment tampering or sabotage);

(ii) Combinations of actions and individual behaviors that appear suspicious and/or dangerous, inappropriate, inconsistent, or out of the ordinary for the employee's work environment, which could indicate a threat to transportation security; and

(iii) How a terrorist or someone with malicious intent may attempt to gain sensitive information or take advantage of vulnerabilities.

(3) *Assess.* Each owner/operator must ensure that each of its security-sensitive employees has knowledge necessary to—

(i) Determine whether the item, individual, behavior, or situation requires a response as a potential terrorist threat based on the respective transportation environment; and

(ii) Identify appropriate responses based on observations and context.

(4) *Respond.* Each owner/operator must ensure that each of its security-sensitive employees has knowledge of how to—

(i) Appropriately report a security threat, including knowing how and when to report internally to other employees, supervisors, or management, and externally to Local, State, or Federal agencies according to the owner/operator's security procedures or other relevant plans;

(ii) Interact with the public and first responders at the scene of the threat or incident, including communication with passengers on evacuation and any specific procedures for individuals with disabilities and the elderly; and

(iii) Use any applicable self-defense devices or other protective equipment provided to employees by the owner/operator.

(g) *Relation to other training.* Training conducted by owner/operators to comply

with other requirements or standards, such as emergency preparedness training required by the Department of Transportation (DOT) (49 CFR part 239) or other training for communicating with emergency responders to arrange the evacuation of passengers, may be combined with and used to satisfy elements of the training requirements in this section.

(h) *Submission.* If commencing or modifying operations subject to these requirements after June 21, 2021, the training program must be submitted to TSA no later than 90 calendar days before commencing new or modified operations.

(i) *Initial security training.* Each owner/operator must provide initial security training to security-sensitive employees, using the curriculum approved by TSA and in compliance with the following schedule.

(1) For security training programs submitted to TSA for approval after March 22, 2021, if the employee is employed to perform a security-sensitive function on the date TSA approves the program, then initial training must be provided no later than 12 months after the date that TSA approves the owner/operator's security training program.

(2) If performance of a security-sensitive job function is initiated after TSA approves the owner/operator's security training program, then initial training must be provided no later than 60 calendar days after the employee first performs the security-sensitive job function.

(3) If the security-sensitive job function is performed intermittently, then initial security training must be provided no later than the 60th calendar day of employment performing a security-sensitive function, aggregated over a consecutive 12-month period.

(j) *Recurrent security training.* (1) Except as provided in paragraph (j)(2) of this section, a security-sensitive employee required to receive training must receive the required training at least once every 3 years.

(2) If an owner/operator modifies a security program or security plan for which

training is required, the owner/operator must ensure each security-sensitive employee with position- or function-specific responsibilities related to the revised plan or program changes receives training on the revisions within 90 days of implementation of the revised plan or program changes. All other employees must receive training that reflects the changes to the operating security requirements as part of their regularly scheduled recurrent training.

(3) The 3-year recurrent training cycle is based on the anniversary calendar month of the employee's initial security training. If the owner/operator provides the recurrent security training in the month of, the month before, or the month after it is due, the employee is considered to have taken the training in the month it is due.

(k) *Recognition of prior training.* Previously provided security training may be credited towards satisfying the requirements of this section provided the owner/operator—

(1) Obtains a complete record of such training and validates the training meets requirements of this section as it relates to the function of the individual security-sensitive employee, and the training was provided within the schedule required for recurrent training; and

(2) Retains a record of such training in compliance with the requirements in paragraph (l).

(l) *Retention of security training records.* The owner/operator must retain records of initial and recurrent security training records for each individual required to receive security training under this section for no less than 5 years from the date of training that, at a minimum—

(1) Includes employee’s full name, job title or function, date of hire, and date of initial and recurrent security training; and

(2) Identifies the date, course name, course length, and list of topics addressed for

the security training most recently provided in each of the areas required under paragraph (e) of this section.

(m) *Availability of records to employees.* The owner/operator must provide records of security training to current and former employees upon request and at no charge as necessary to provide proof of training.

(n) *Incorporation into security program.* Once approved by TSA, the security training program required by this section is part of the owner/operator's TSA-approved security program. The owner/operator must implement and maintain the security training program and comply with timeframes for implementation identified in the security training program. Any modifications or amendments to the program must be made as stipulated in § 1570.107 of this subchapter.

(o) *Situations requiring owner/operator to revise security training program.* The owner/operator must submit a request to amend its security program if, after approval, the owner/operator makes, or intends to make, permanent (to be in effect for 60 or more calendar days) or substantive changes to its security training curriculum, including changes to address:

(1) Determinations that the security training program is ineffective based on the approved method for evaluating effectiveness in the security training program approved by TSA; or

(2) Development of recurrent training material for purposes of meeting the requirements in paragraph (j) of this section or other alternative training materials not previously approved by TSA.

§ 1582.115 [Reserved]

24. Add subpart C of part 1582 to read as follows:

Subpart C—Cybersecurity Risk Management

Sec.
§ 1582.201 Scope and applicability.

§ 1582.203 Form, content, and availability of Cybersecurity Risk Management program.
§ 1582.205 Cybersecurity evaluation.
§ 1582.207 Cybersecurity Operational Implementation Plan.
§ 1582.209 Governance of the CRM program.
§ 1582.211 Cybersecurity Coordinator.
§ 1582.213 Identification of Critical Cyber Systems.
§ 1582.215 Supply chain risk management.
§ 1582.217 Protection of Critical Cyber Systems.
§ 1582.219 Cybersecurity training and knowledge.
§ 1582.221 Detection of cybersecurity incidents.
§ 1582.223 Capabilities to respond to a cybersecurity incident.
§ 1582.225 Reporting cybersecurity incidents.
§ 1582.227 Cybersecurity Incident Response Plan.
§ 1582.229 Cybersecurity Assessment Plan
§ 1582.231 Documentation to establish compliance.

§ 1582.201 Scope and applicability.

(a) *Scope.* This subpart includes requirements to ensure the cybersecurity of public transportation and passenger railroads to mitigate the risk of significant harm to individuals and transportation facilities, as well as persons in areas in or near rail operations, that could have their safety and security threatened as a result of the degradation, destruction, or malfunction of systems that control these systems and infrastructure. In addition, cybersecurity incidents could have significant impacts on national and economic security of the United States by impeding the movement of people who rely on public transportation for commuting or intercity rail operations. The owner/operators identified in § 1582.1 must review the applicability for carrying out a Cybersecurity Risk Management program in paragraph (b) of this section, designation of a Cybersecurity Coordinator in § 1582.211, and reporting cybersecurity requirements in § 1582.225 to determine if the requirements apply to their operations.

(b) *Applicability.* Each owner/operator described in § 1582.1 must adopt and carry out a Cybersecurity Risk Management (CRM) program for each operation that meets any of the following criteria:

(1) Is a passenger railroad carrier with average daily unlinked passenger trips of 5,000 or greater in any of the three calendar years before [EFFECTIVE DATE OF

FINAL RULE] or any single calendar year after [EFFECTIVE DATE OF FINAL RULE].

(2) Is a passenger railroad carrier described in § 1582.1(a)(1) through (3) that serves as a host railroad to a class I railroad or Amtrak, regardless of ridership volume.

(3) Is a rail transit system described in § 1582.1(a)(3) with average daily unlinked passenger trips of 50,000 or greater in any of the three calendar years before [EFFECTIVE DATE OF FINAL RULE] or any single calendar year after [EFFECTIVE DATE OF FINAL RULE].

§ 1582.203 Form, content, and availability of Cybersecurity Risk Management program.

(a) *General content requirements*. The CRM program required by this subpart is a comprehensive program that includes the following components:

(1) A cybersecurity evaluation completed and updated as required by § 1582.205;

(2) A TSA-approved Cybersecurity Operational Implementation Plan (COIP) that meets the requirements in § 1582.207.

(3) A Cybersecurity Assessment Plan that meets the requirements in § 1582.229.

(b) *Subsidiaries.* If a single CRM program is developed and implemented for multiple business units within a single corporate entity, any documents used to comply or establish compliance with the requirements in this subpart must clearly identify and distinguish application of the requirements to each business unit.

§ 1582.205 Cybersecurity evaluation.

(a) *General.* Each owner/operator required to have a CRM program must complete an initial and recurrent cybersecurity evaluation sufficient to determine the owner/operator's current enterprise-wide cybersecurity profile of logical/virtual and physical security controls when evaluated against the CRM program requirements in this subpart, using a form provided by TSA or other tools approved by TSA.

(b) *Timing.* The initial cybersecurity evaluation must be completed no later than [DATE 90 DAYS AFTER EFFECTIVE DATE OF FINAL RULE], but no more than one year before the date of submission of the owner/operator's Cybersecurity Operational Implementation Plan required by § 1582.207 of this subpart. If commencing or modifying operations subject to these requirements after [EFFECTIVE DATE OF FINAL RULE], the initial cybersecurity evaluation must be submitted to TSA no later than 45 calendar days after commencing the new or modified operations triggering applicability.

(c) *Annual updates.* The evaluation required by paragraph (a) of this section must be updated annually, no later than one year from the anniversary date of the previously completed evaluation.

(d) *Notification.* The owner/operator must notify TSA within 7 days of completing the evaluation and annual updates required by this section. A copy of the evaluation must be provided to TSA upon request.

(e) *Sensitive Security Information.* This evaluation is a vulnerability assessment as defined in § 1500.3 of this chapter and must be protected as Sensitive Security Information under § 1520.5(b)(5) of this chapter.

§ 1582.207 Cybersecurity Operational Implementation Plan.

(a) *Requirement.* Each owner/operator required to have a CRM program under this part must adopt a COIP.

(b) *General Content.* The COIP must include the following corporate information:

(1) The name and corporate address of the owner/operator;

(2) Written attestation by the owner/operator's accountable executive that the COIP has been reviewed and approved by senior management; and

(3) Identification of specific operations that meet the applicability criteria.

(c) *Specific Content.* The COIP must detail the owner/operator's defense-in-depth plan, including physical and logical/virtual security controls, to comply with the requirements and security outcomes specified in the following sections:

(1) *Governance.* The requirements for governance of the CRM program in § 1582.209 and the designation of a Cybersecurity Coordinator in § 1582.211.

(2) *Identification of Critical Cyber Systems, Network Architecture, and Interdependencies.* The requirements to identify Critical Cyber Systems and network architecture in § 1582.213 and supply chain risk management in § 1582.215.

(3) *Procedures, policies, and capabilities to protect Critical Cyber Systems.* The requirements for protection of Critical Cyber Systems in § 1582.217 and training of cybersecurity-sensitive employees in § 1582.219.

(4) *Procedures, policies, and capabilities to detect cybersecurity incidents.* The requirements for detecting cybersecurity incidents in § 1582.221.

(5) *Procedures, policies, and capabilities to respond to, and recover from, cybersecurity incidents.* The requirements for responding to cybersecurity incidents in § 1582.223, reporting cybersecurity incidents in § 1582.225, and the Cybersecurity Incident Response Plan in § 1582.227.

(d) *Plan of Action and Milestones.* (1) To the extent an owner/operator does not meet every requirement and security outcome identified in paragraph (c)(1) through (c)(5) of this section, the COIP must include a plan of action and milestones (POAM).

(2) The POAM must include:

(i) Policies, procedures, measures, or capabilities that owner/operator will develop or obtain, as applicable, to ensure all requirements and security outcomes in this subpart are met;

(ii) Physical and logical/virtual security controls that the owner/operator will implement to mitigate the risks associated with not fully complying with requirements or

security outcomes in this subpart; and

(iii) A detailed timeframe for full compliance with all requirements and security outcomes in this subpart, not to exceed 3 years from the date of submission to TSA of the COIP required by this section.

(3) The POAM must be updated as necessary to address any deficiencies identified during the evaluation required by § 1582.205 or because of an assessment conducted under § 1582.229 that will not be immediately addressed through an update to the COIP.

(e) *Approval and implementation.* (1) *Submission deadlines.* The COIP must be made available to TSA, in a form and manner prescribed by TSA, no later than [DATE 180 DAYS AFTER EFFECTIVE DATE OF FINAL RULE]. If commencing or modifying operations subject to these requirements after [EFFECTIVE DATE OF FINAL RULE], the COIP must be made available to TSA no later than 45 calendar days before commencing new or modified operations.

(2) *Effective date.* After considering all relevant materials and any additional information required by TSA, TSA will notify the owner/operator's accountable executive of TSA's decision to approve the owner/operator's COIP. The COIP becomes effective 30 days after the owner/operator is notified whether its COIP is approved.

(3) *TSA-approved security program.* Once approved by TSA, the COIP, any appendices, and any policies or procedures incorporated by reference, are a part of a TSA-approved security program, subject to the protections in part 1520 of this chapter and the procedures applicable to security programs in subpart B of part 1570 of this subchapter.

(f) *Status Report and Updates.* The CRM program must be reviewed and updated by the owner/operator within 60 days of the evaluations or assessments required by §§ 1582.205 or 1582.229, as necessary to address any identified vulnerabilities or

weaknesses in the procedures, policies, or capabilities identified in the CRM program.

(g) *Revisions.* Unless otherwise specified in this subpart, any substantive modifications or amendments to the COIP must be made in accordance with the procedures in § 1570.107 of this subchapter.

§ 1582.209 Governance of the CRM program.

(a) *Accountable Executive.* (1) No later than [DATE 30 DAYS FROM EFFECTIVE DATE OF FINAL RULE], the owner/operator must provide to TSA the names, titles, business telephone numbers, and business email addresses of the owner/operator's accountable executive and the primary individual to be contacted about the owner/operator's CRM program. If any of the information required by this section changes, the owner/operator must provide the updated information to TSA within seven days of the change.

(2) The accountable executive must be an individual who has the authority and knowledge necessary for the development, implementation, and managerial oversight of the TSA-approved CRM program, including cybersecurity administration, risk assessments, inspections and control procedures, and coordinating communications with the owner/operator's leadership and staff on implementation and sustainment of the CRM program. To the extent possible, the accountable executive should not be the Cybersecurity Coordinator or an individual responsible for management of Information or Operational Technology system or systems' administration.

(b) *COIP.* The COIP must also include:

(1) Identification of positions designated by the owner/operator to manage implementation of policies, procedures, and capabilities described in the COIP and coordinate improvements to the CRM program.

(2) Corporate-level identification of any authorized representatives, as defined in the TSA Cybersecurity Lexicon, who are responsible for any or all the CRM program or

cybersecurity measures identified in the CRM program, and written documentation (such as contractual agreements) clearly identifying the roles and responsibilities of the authorized representative under the CRM program.

(3) The information required by paragraph (a)(1) of this section.

(c) *Process.* Updating the COIP to align with information provided to TSA under this section does not require an amendment subject to the procedures in § 1570.107 of this subchapter.

§ 1582.211 Cybersecurity Coordinator.

(a)(1) Except as provided in paragraph (a)(2), each owner/operator identified in paragraphs § 1582.103(a) must designate employees at the corporate level to serve as the primary and at least one alternate Cybersecurity Coordinator with responsibility for sharing critical cybersecurity information.

(2) Each owner/operator identified in § 1582.103(a)(3) must designate and use a primary and at least one alternate Cybersecurity Coordinator only if notified by TSA in writing that a threat exists concerning that type of operation.

(b) The Cybersecurity Coordinator and alternate(s) must—

(1) Serve as the primary contact for cyber-related intelligence information and cybersecurity-related activities and communications with TSA and the Cybersecurity and Infrastructure Security Agency (CISA);

(2) Have the following knowledge and skills, through current certifications or equivalent job experience:

(i) General cybersecurity guidance and best practices;

(ii) Relevant law and regulations pertaining to cybersecurity;

(iii) Handling of Sensitive Security Information and security-related communications; and

(iv) Current cybersecurity threats applicable to the owner/operator’s operations

and systems.

(3) Be accessible to TSA and CISA 24 hours per day, seven days per week;

(4) Have a Homeland Security Information Network (HSIN) account or other TSA-designated communication platform for information sharing relevant to the requirements in this subpart; and

(5) Work with appropriate law enforcement and emergency response agencies in addressing cybersecurity threats or responding to cybersecurity incidents.

(c) The Cybersecurity Coordinator and alternate(s) must be a U.S. citizen eligible for a security clearance, unless otherwise waived by TSA.

(d) Owner/operators must provide in writing to TSA the names, titles, business phone number(s), and business email address(es) of the Cybersecurity Coordinator and alternate Cybersecurity Coordinator(s) required by paragraph (a) no later than [DATE 7 DAYS AFTER EFFECTIVE DATE OF FINAL RULE], or within 7 days of the commencement of new operations, or change in any of the information required by this section that occur after [DATE 7 DAYS AFTER EFFECTIVE DATE OF FINAL RULE].

(e) In addition to providing the information to TSA as required by paragraph (d), any owner/operator required to have a CRM program under this part must also include the information required by paragraphs (d) of this section in the COIP. As the owner/operator must separately notify TSA of this information, and any changes to this information, updating the COIP to align with information provided to TSA under this section does not require an amendment subject to the procedures in § 1570.107 of this subchapter.

§ 1582.213 Identification of Critical Cyber Systems.

(a) *Identifying information.* The owner/operator must incorporate into its COIP a list of Critical Cyber Systems, as defined in the TSA Cybersecurity Lexicon, that

provides, at a minimum, the following identifying information for each Critical Cyber System:

(1) Identifier (system name or commercial name); and

(2) System manufacturer/designer name.

(b) *Identification methodology.* The owner/operator must include a description of the methodology and information used to identify Critical Cyber Systems that, at a minimum, includes the following information as used to identify critical systems:

(1) Standards and factors, including system interdependencies with critical functions, used to identify Information Technology and Operational Technology systems that could be vulnerable to a cybersecurity incident;

(2) Sources and data, such as known threat information relevant to the system, that informed decisions regarding the likelihood of the system being subject to a cybersecurity incident;

(3) Potential operational impacts of a cybersecurity incident, including scenarios that identify potential supply chain impacts and how long critical operations and capabilities could be sustained with identified alternatives if a system is offline; and

(4) Sustainability and operational impacts if an Information or Operational Technology system not identified as a Critical Cyber System becomes unavailable due to a cybersecurity incident.

(c) *Positive Train Control (PTC) Systems.* Owner/operators who are either required to install and operate PTC under 49 CFR part 236, subpart I, and/or voluntarily install and operate PTC under CFR part 236, subpart H or I, must include PTC systems as a Critical Cyber System.

(d) *System information and network architecture.* For all Critical Cyber Systems, the owner/operator must provide the following information:

(1) Information and Operational Technology system interdependencies for

Critical Cyber Systems;

(2) All external connections to Critical Cyber Systems;

(3) Zone boundaries for Critical Cyber Systems, including a description of how Information and Operational Technology systems are defined and organized into logical/virtual zones based on criticality, consequence, and operational necessity;

(4) Baseline of acceptable communications between Critical Cyber Systems and external connections or between Information and Operational Technology systems; and

(5) Operational needs that prevent or delay implementation of the requirements in this subpart, such as application of security patches and updates, encryption of communications traversing Information and Operational Technology systems, and multi-factor authentication.

(e) *Additional systems.* If notified by TSA, the owner/operator must include additional Critical Cyber Systems identified by TSA not previously identified by the owner/operator.

(f) *Changes in Critical Cyber Systems.* Any substantive changes to Critical Cyber Systems require an amendment to the Cybersecurity Operational Implementation Plan subject to the procedures in § 1570.107 of this subchapter.

§ 1582.215 Supply chain risk management.

The owner/operator must incorporate into its COIP policies, procedures, and capabilities to address supply chain cybersecurity vulnerabilities that include requiring—

(a) All procurement documents and contracts, including service-level agreements, executed or updated after [EFFECTIVE DATE OF FINAL RULE], include a requirement for the vendor or service provider to notify the owner/operator of the following:

(1) Cybersecurity incidents affecting the vendor or service provider within a specified timeframe sufficient for the owner/operator to identify and address any

potential risks to their Critical Cyber Systems based on the scope and type of cybersecurity incident.

(2) Confirmed security vulnerabilities affecting the goods, services, or capabilities provided by the vendor or service provider within a specified timeframe sufficient for the owner/operator to identify and address any potential risks to their Critical Cyber Systems based on the scope and type of security vulnerability.

(b) Procurement documents and contracts, including service-level agreements, incorporate an evaluation by the owner/operator or qualified third-party of the cybersecurity measures implemented by vendors or service providers of goods, services, or capabilities that will be connected to, installed on, or used by the owner/operator's Critical Cyber Systems.

(c) When provided two offerings of roughly similar cost and function, giving preference to the offering that provides the greater level of cybersecurity necessary to protect against, or effectively respond to, cybersecurity incidents affecting the owner/operator's Critical Cyber Systems.

(d) Upon notification of a cybersecurity incident or vulnerability under paragraphs (a) or (b) of this section, immediate consideration of mitigation measures sufficient to address the resulting risk to Critical Cyber Systems and, as applicable, revision to the COIP in accordance with § 1570.107 of this subchapter.

§ 1582.217 Protection of Critical Cyber Systems.

The owner/operator must incorporate into its COIP policies, procedures, controls, and capabilities to protect Critical Cyber Systems that meet security performance objectives in the following areas—

(a) *Network segmentation.* Network segmentation measures that protect against access to, or disruption of, the Operational Technology system if the Information Technology system is compromised or vice versa. These measures must be sufficient

to—

(1) Ensure Information and Operational Technology system-services transit the other only when necessary for validated business or operational purposes;

(2) Secure and defend zone boundaries with security controls—

(i) To defend against unauthorized communications between zones; and

(ii) To prohibit Operational Technology system services from traversing the Information Technology system, and vice-versa, unless the content is encrypted at a level sufficient to secure and protect integrity of data and prevent corruption or compromise while in transit. If encryption is not technologically feasible, ensure content is otherwise secured and protected using compensating controls that provide the same level of security as encryption for data in transit.

(b) *Access control.* Access control measures for Critical Cyber Systems, including for local and remote access, that secure and defend against unauthorized access to Critical Cyber Systems. Except as provided in paragraph (f), these measures must, at a minimum, incorporate the following policies, procedures, and controls:

(1) Identification and authentication requirements designed to prevent unauthorized access to Critical Cyber Systems that include:

(i) A policy for memorized secret authenticator resets that includes criteria for passwords and when resets must occur, including procedures to ensure implementation of these requirements, such as password lockouts; and

(ii) Documented and defined logical/virtual and physical security controls for components of Critical Cyber Systems that will not be subject to the requirements in paragraph (b)(1)(i) of this section.

(2) Multi-factor authentication, or other logical/virtual and physical security controls to supplement memorized secret authenticators (such as passwords) to provide risk mitigation commensurate to multi-factor authentication. If an owner/operator does

not apply multi-factor authentication for access to Operational Technology components or assets, the owner/operator must specify what compensating controls are used to manage access.

(3) Management of access rights based on the principles of least privilege and separation of duties. Where not technically feasible to apply these principles, the policies and procedures must describe compensating controls that the owner/operator applies.

(4) Policies and procedures limit availability and use of shared accounts to those that are critical for operations, and then only if necessary. When the owner/operator uses shared accounts for operational purposes, the policies and procedures must ensure:

(i) Access to shared accounts is limited through account management that uses principles of least privilege and separation of duties;

(ii) Any individual who no longer needs access does not have knowledge of the memorized secret authenticator necessary to access the shared account; and

(iii) Logs are maintained sufficient to enable positive user identification of access to shared accounts to enable forensic investigation following a cybersecurity incident.

(5) Regularly updated schedule for review of existing domain trust relationships to ensure their necessity and established and enforced policies to manage these relationships.

(c) *Patch management.* Measures that reduce the risk of exploitation of unpatched systems through the application of security patches and updates for operating systems, applications, drivers, and firmware on Critical Cyber Systems consistent with the owner/operator's risk-based methodology. These measures must include:

(1) A patch management strategy that ensures all critical security patches and updates on Critical Cyber Systems are current. This strategy must include:

(i) The risk methodology for categorizing and determining criticality of patches and updates, and an implementation timeline based on categorization and criticality; and

(ii) Prioritization of all security patches and updates on CISA's Known Exploited Vulnerabilities Catalog.

(2) In instances where the owner/operator cannot apply patches and updates on specific Operational Technology systems without causing a severe degradation of operational capability to meet business critical functions, the owner/operator must provide an explanation for why the actions cannot be taken and a description and timeline of additional mitigations that address the risk created by not installing the patch or update within the recommended timeframe.

(d) *Logging policies.* Logging policies sufficient to ensure logging data is—

(1) Stored in a secure and centralized system, such as a security information and event management tool or database on a segmented network that can only be accessed or modified by authorized and authenticated users; and

(2) Maintained for a duration sufficient to allow for investigation of cybersecurity incidents as supported by a risk analysis and applicable standards or regulatory guidelines.

(e) *Secure back-ups.* Policies that ensure all Critical Cyber Systems are backed-up on a regular basis consistent with operational need for the information, the back-ups are securely stored separate from the system, and policies require testing the integrity of back-ups to ensure that the data is free of known malicious code when the back-ups are made.

(f) *Exception for PTC hardware and software components installed on locomotive.* (1) For hardware and software components of a PTC system installed on a locomotive, owner/operators in compliance with requirements in 49 CFR 232.105(h)(1-4) (General requirements for locomotives), 49 CFR 236.3 (Locking of signal apparatus housings), and 49 CFR 256.553 (Seal, where required), may rely on the physical security measures used to comply with these requirements, as applicable, in lieu of implementing

the requirements in paragraph (b).

(2) If relying on the exception in paragraph (f)(1), the owner/operator must list the applicable PTC system as a Critical Cyber System; maintain compliance with the requirements specified in 49 CFR 232.105(h)(1-4), 49 CFR 236.3, and 49 CFR 256.553, as applicable; and include in the COIP a description of the physical security measures used to prevent unauthorized access to the identified PTC components.

§ 1582.219 Cybersecurity training and knowledge.

(a) *Training required.* (1) Owner/operators required to have a CRM program under this subpart must provide basic cybersecurity training to all employees with access to the owner/operator's Information or Operational Technology systems.

(2) No owner/operator required to have a CRM program under this subpart may permit a cybersecurity-sensitive employee to access, or have privileges to access, a Critical Cyber System or an Information or Operational Technology system that is interdependent with a Critical Cyber System, unless that individual has received basic and role-based cybersecurity training.

(b) *General curriculum requirements.* The cybersecurity training program must include a curriculum or lesson plan, including learning objectives and method of delivery (such as instructor-led or computer-based training) for each course used to meet the requirements in paragraphs (d) and (e) of this section. TSA may request additional information regarding the curriculum during the review and approval process. If recurrent training under paragraph (e) of this section is not the same as initial training, a curriculum or lesson plan for the recurrent training will need to be submitted and approved by TSA.

(c) *Specific curriculum requirements.* (1) *Basic cybersecurity training.* All employees and contractors with access to the owner/operator's Information or Operational Technology systems, must receive basic cybersecurity training that includes

cybersecurity awareness to address best practices, acceptable use, risks associated with their level of privileged access, and awareness of security risks associated with their actions. This training must address the following topics:

(i) Social engineering, including phishing;

(ii) Password best practices;

(iii) Remote work security basics;

(iv) Safe internet and social media use;

(v) Mobile device (wireless) vulnerabilities and network security;

(vi) Data management and information security, including protecting business email, confidential information, trade secrets, and privacy; and

(vii) How and to whom to report suspected inappropriate or suspicious activity involving Information or Operational Technology systems, including mobile devices provided by or connected to the owner/operator's Information or Operational Technology systems.

(2) *Role-based cybersecurity training.* Cybersecurity-sensitive employees must be provided cybersecurity training that specifically addresses their role as a privileged user to prevent and respond to a cybersecurity incident, acceptable uses, and the risks associated with their level of access and use as approved by the owner/operator. This training must address the following topics as applicable to the specific role:

(i) Security measures and requirements in the COIP including how the requirements affect account and access management, server and application management, and system architecture development and assessment;

(ii) Recognition and detection of cybersecurity threats, types of cybersecurity incidents, and techniques used to circumvent cybersecurity measures;

(iii) Incident handling, including procedures for reporting a cybersecurity incident to the Cybersecurity Coordinator and understanding their roles and responsibilities during

a cybersecurity incident and implementation of the owner/operator's Cybersecurity Incident Response Plan required by § 1582.227;

(iv) Requirements and sources for staying aware of changing cybersecurity threats and countermeasures;

(v) Operational Technology-specific cybersecurity training for all personnel whose duties include access to Operational Technology systems.

(d) *Initial cybersecurity training.* (1) Each owner/operator must provide initial cybersecurity training (basic and role-based, as applicable) to employees and contractors, using the curriculum approved by TSA no later than 60 days after the effective date of the owner/operator's TSA-approved COIP required by this subpart.

(2) For individuals who onboard or become cybersecurity-sensitive employees after the effective date of the owner/operator's TSA-approved COIP who did not receive training within the period identified in paragraph (d)(1) of this section, the individual must receive the applicable cybersecurity training no later than 10 days after onboarding.

(e) *Recurrent cybersecurity training.* Employees and contractors must receive annual recurrent cybersecurity training no later than the anniversary calendar month of the employee's initial cybersecurity training. If the owner/operator provides the recurrent cybersecurity training in the month of, the month before, or the month after it is due, the employee is considered to have taken the training in the month it is due.

(f) *Recognition of prior or established cybersecurity training.* Previously provided cybersecurity training may be credited towards satisfying the requirements of this section provided the owner/operator—

(1) Obtains a complete record of such training and validates the training meets requirements of this section as it relates to the role of the individual employee, and the training was provided within the schedule required for recurrent training; and

(2) Retains a record of such training in compliance with the requirements in

paragraph (g) of this section.

(g) *Retention of cybersecurity training records.* The owner/operator must retain records of initial and recurrent cybersecurity training records for each individual required to receive cybersecurity training under this section for no less than 5 years from the date of training that, at a minimum—

(1) Includes employee's full name, job title or function, date of hire, and date of initial and recurrent cybersecurity training; and

(2) Identifies the date, course name, course length, and list of topics addressed for the cybersecurity training most recently provided in each of the areas required under paragraph (c) of this section.

(h) *Availability of records to employees.* The owner/operator must provide records of cybersecurity training to current and former employees upon request and at no charge as necessary to provide proof of training.

§ 1582.221 Detection of cybersecurity incidents.

The owner/operator must incorporate into its COIP policies, procedures, and capabilities sufficient to detect and respond to cybersecurity threats to, and anomalies on, Critical Cyber Systems that, at a minimum—

(a) Defend against malicious email, such as spam and phishing emails, to preclude or mitigate against adverse impacts to operations;

(b) Block ingress and egress communications with known or suspected malicious Internet Protocol addresses;

(c) Control impact of known or suspected malicious web domains or web applications, such as by preventing users and devices from accessing malicious websites;

(d) Block and defend against unauthorized code, including macro scripts, from executing;

(e) Monitor and/or block connections from known or suspected malicious

command and control servers (such as Tor exit nodes, and other anonymization services); and

(f) Ensure continuous collection and analysis of data for potential intrusions and anomalous behavior on Critical Cyber Systems and other Information and Operational Technology systems that directly connect with Critical Cyber Systems.

§ 1582.223 Capabilities to respond to a cybersecurity incident.

The owner/operator must incorporate into its COIP capabilities to respond to cybersecurity incidents affecting Critical Cyber Systems that, at a minimum—

(a) Audit unauthorized access to internet domains and addresses;

(b) Document and audit any communications between the Operational Technology system and an internal or external system that deviates from the owner/operator's identified baseline of communications;

(c) Identify and respond to execution of unauthorized code, including macro scripts; and

(d) Define, prioritize, and drive standardized incident response activities, such as Security Orchestration, Automation, and Response (SOAR).

§ 1582.225 Reporting cybersecurity incidents.

(a)(1) Except as provided in paragraph (a)(2) of this section or otherwise directed by TSA, each owner/operator identified in § 1582.1 must notify CISA of any Reportable Cybersecurity Incidents, as defined in the TSA Cybersecurity Lexicon, as soon as practicable, but no later than 24 hours after a Reportable Cybersecurity Incident is identified.

(2) An owner/operator identified in § 1582.1(a)(2) that owns or operates a bus-only operation must notify CISA of Reportable Cybersecurity Incidents under paragraph (a)(1) only if the owner/operator is identified in appendix A to part 1582 of this subchapter or is notified by TSA in writing that a threat exists concerning that operation.

(b) Reports required by this section must be made by the methods prescribed by TSA. All reported information will be protected in a manner appropriate for the sensitivity and criticality of the information.

(c) The report to CISA must include the following information, as available to the reporting owner/operator at the time of the report:

(1) The name of the reporting individual and contact information, including a telephone number and email address. The report must also explicitly specify that the information is being reported to satisfy the reporting requirements in Transportation Security Regulations.

(2) The affected conveyance, system(s) or facilities, including identifying information and location.

(3) Description of the threat, incident, or activity, to include:

(i) Earliest known date of compromise;

(ii) Date of detection;

(iii) Information about who has been notified and what action has been taken;

(iv) Any relevant information observed or collected by the owner/operators, such as malicious Internet Protocol addresses, malicious domains, malware hashes and/or samples, or the abuse of legitimate software or accounts; and

(v) Any known threat information, to include information about the source of the threat or cybersecurity incident, if available.

(4) A description of the incident's impact or potential impact on Information or Operational Technology systems and operations. This information must also include an assessment of actual or imminent adverse impacts to service operations, operational delays, and/or data theft that have or are likely to be incurred, as well as any other information that would be informative in understanding the impact or potential impact of the cybersecurity incident.

(5) A description of all responses that are planned or under consideration, to include, for example, a reversion to manual operations of train movement and control, if applicable.

(6) Any additional information not specifically required by this section, but which is critical to an understanding of the threat and owner/operator's response to a reportable cybersecurity incident.

(d) If all the required information is not available at the time of reporting, owner/operators must submit an initial report within the specified timeframe and supplement as additional information becomes available.

§ 1582.227 Cybersecurity Incident Response Plan.

(a) The owner/operator must incorporate into its COIP an up-to-date Cybersecurity Incident Response Plan (CIRP) for the owner/operator's Critical Cyber Systems to reduce the impacts of a cybersecurity incident that causes, or could cause, operational disruption or significant impacts on business-critical functions.

(b) The CIRP must provide specific measures sufficient to ensure the following objectives, as applicable:

(1) Promptly identifying, isolating, and segregating the infected systems from uninfected systems, networks, and devices using measures that prioritize:

(i) Limiting the spread of autonomous malware;

(ii) Denying continued access by a threat actor to systems;

(iii) Determining extent of compromise; and

(iv) Preserving evidence and data.

(2) Only data stored and secured as required by § 1582.217(e) is used to restore systems and that all stored backup data is scanned with host security software to ensure the data is free of malicious artifacts before being used for restoration.

(3) Established capability and governance for implementing mitigation measures

or manual controls that ensure that the Operational Technology system can be isolated when a cybersecurity incident in the Information Technology system creates risk to the safety and reliability of the Operational Technology system.

(c) The CIRP must identify who (by position) is responsible for implementing the specific measures in the plan and any necessary resources needed to implement the measures.

(d) The owner/operator must conduct an exercise to test the effectiveness of the CIRP no less than annually. The exercise conducted under this paragraph must—

(1) Test at least two objectives of the owner/operator's CIRP required by paragraph (b) of this section, no less than annually; and

(2) Include the employees identified (by position) in paragraph (c) as active participants in the exercise.

(e) Within no more than 90 days after the date of the exercise required by paragraph (d), the owner/operator must update the CIRP as appropriate to address any issues identified during the exercise.

(f) The owner/operator must notify TSA within 15 days of any changes to the CIRP. As the owner/operator must separately notify TSA, updating the COIP to align with information provided to TSA under this section does not require an amendment subject to the procedures in § 1570.107 of this subchapter.

§ 1582.229 Cybersecurity Assessment Plan

(a) *Requirement for a Cybersecurity Assessment Plan.* No later than 90 days from TSA's approval of the owner/operator's COIP, the owner/operator must submit to TSA a Cybersecurity Assessment Plan (CAP) sufficient to—

(1) Proactively assess the effectiveness of all policies, procedures, measures, and capabilities in the owner/operator's TSA-approved COIP as applied to all Critical Cyber Systems; and

(2) Identify and resolve device, network, and/or system vulnerabilities associated with Critical Cyber Systems.

(b) *Contents of the CAP.* At a minimum, the CAP must describe in detail:

(1) The plan to assess the effectiveness of the owner/operator's TSA-approved COIP as applied to all Critical Cyber Systems;

(2) Schedule and scope of an architectural design review within 12 months either before or after TSA's approval of the owner/operator's COIP, to be repeated at least once every 2 years thereafter. The architectural design review required by this paragraph must include verification and validation of network traffic, a system log review, and analysis to identify cybersecurity vulnerabilities related to network design, configuration, and interconnectivity to internal and external systems;

(3) Other assessment capabilities designed to identify vulnerabilities to Critical Cyber Systems based on evolving threat information and adversarial capabilities, such as penetration testing of Information Technology systems, including the use of "red" and "purple" team (adversarial perspective) testing.

(c) *Specific Schedule.* (1) In addition to specifying the schedule for the architectural design review required by paragraph (b)(2), the CAP must include a schedule for conducting the assessments required by paragraph (b) sufficient to ensure at least one-third of the policies, procedures, measures, and capabilities in the TSA-approved COIP are assessed each year, with 100 percent of the COIP and all Critical Cyber Systems assessed over a 3-year period.

(2) The scheduled required by this paragraph must map the planned assessments to the COIP and Critical Cyber System to document the plan will ensure all policies, procedures, measures, and capabilities in the owner/operator's TSA-approved COIP and all Critical Cyber Systems will be assessed within the timeframes required by paragraph (c)(1).

(d) *Independence of assessors and auditors.* Owner/operators must ensure that the assessments, audits, testing, and other capabilities to assess the effectiveness of its TSA-approved COIP are not conducted by individuals who have oversight or responsibility for implementing the owner/operators CRM program and have no vested or other financial interest in the results of the CAP.

(e) *Annual submission of report.* The owner/operator must ensure a report of the results of assessments conducted in accordance with the CAP is provided to corporate leadership and individuals designated under § 1582.209(a) and (b)(1) of this subpart, and submitted to TSA, no later than 15 months from the date of approval of the initial CAP and annually thereafter. The required report must indicate—

(1) Which assessment method(s) were used to determine if the policies, procedures, and capabilities described by the owner/operator in its COIP are effective; and

(2) Results of the individual assessment methodologies.

(f) *Annual update of the CAP.* The owner/operator must review and annually update the CAP to address any changes to policies, procedures, measures, or capabilities in the COIP or assessment capabilities required by paragraph (b). The updated CAP must be submitted to TSA for approval no later than 12 months from the date of TSA's approval of the current CAP.

(g) Assessments conducted under this section are vulnerability assessments as defined in 1500.3 of his chapter and must be protected as Sensitive Security Information under § 1520.5(b)(5) of this chapter.

§ 1582.231 Documentation to establish compliance.

For the purposes of the requirements in this subpart, upon TSA's request, the owner/operator must provide for inspection or copying the following types of information to establish compliance:

(a) Hardware/software asset inventory, including supervisory control and data acquisition (SCADA) systems;

(b) Firewall rules;

(c) Network diagrams, switch and router configurations, architecture diagrams, publicly routable internet protocol addresses, and Virtual Local Area Networks;

(d) Policy, procedural, and other documents that informed the development, and documented implementation of, the owner/operator's CRM program;

(e) Data providing a "snapshot" of activity on and between Information and Operational Technology systems such as:

(1) Log files;

(2) A capture of network traffic (such as packet capture (PCAP)), for a scope and period directed by TSA, not less than 24 hours and not to exceed 48 hours;

(3) "East-West Traffic" of Information Technology systems, sites, and environments within the scope of this subpart; and

(4) "North-South Traffic" between Information and Operational Technology systems, and the perimeter boundaries between them; and

(f) Any other records or documents necessary to determine compliance with this subpart.

25. Revise appendix B to part 1582 to read as follows:

Appendix B to Part 1582—Security-Sensitive Job Functions for Public Transportation and Passenger Railroads

This table identifies security-sensitive job functions for owner/operators regulated under this part. All employees performing security-sensitive functions are "security-sensitive employees" for purposes of this rule and must be trained in accordance with this part.

Categories	Security-Sensitive Job Functions for Public Transportation and Passenger Railroads (PTPR)

A. Operating a vehicle ……..	1. Employees who— a. Operate or control the movements of trains, other rail vehicles, or transit buses. b. Act as train conductor, trainman, brakeman, or utility employee or performs acceptance inspections, couples and uncouples rail cars, applies handbrakes, or similar functions. 2. Employees covered under the Federal hours of service laws as "train employees." *See* 49 U.S.C. 21101(5) and 21103.
B. Inspecting and maintaining vehicles ……..	Employees who— 1. Perform activities related to the diagnosis, inspection, maintenance, adjustment, repair, or overhaul of electrical or mechanical equipment relating to vehicles, including functions performed by mechanics and automotive technicians. 2. Provide cleaning services to vehicles owned, operated, or controlled by an owner/operator regulated under this subchapter.
C. Inspecting or maintaining building or transportation infrastructure ……	Employees who— 1. Maintain, install, or inspect communication systems and signal equipment related to the delivery of transportation services. 2. Maintain, install, or inspect track and structures, including, but not limited to, bridges, trestles, and tunnels. 3. Provide cleaning services to stations and terminals owned, operated, or controlled by an owner/operator regulated under this subchapter that are accessible to the general public or passengers. 4. Provide maintenance services to stations, terminals, yards, tunnels, bridges, and operation control centers owned, operated, or controlled by an owner/operator regulated under this subchapter. 5. Employees covered under the Federal hours of service laws as "signal employees." *See* 49 U.S.C. 21101(4) and 21104.
D. Controlling dispatch or movement of a vehicle ……...	Employees who— 1. Dispatch, report, transport, receive or deliver orders pertaining to specific vehicles, coordination of transportation schedules, tracking of vehicles and equipment. 2. Manage day-to-day management delivery of transportation services and the prevention of, response to, and redress of service disruptions. 3. Supervise the activities of train crews, car movements, and switching operations in a yard or terminal. 4. Dispatch, direct, or control the movement of trains or buses. 5. Operate or supervise the operations of moveable bridges. 6. Employees covered under the Federal hours of service laws as "dispatching service employees." *See* 49 U.S.C. 21101(2) and 21105.
E. Providing security of the owner/operator's equipment and property ……	Employees who— 1. Provide for the security of PTPR equipment and property, including acting as a police officer. 2. Patrol and inspect property of an owner/operator regulated under subchapter to protect the property, personnel, passengers and/or cargo.
F. Loading or unloading cargo or baggage ……	Employees who load, or oversee loading of, property tendered by or on behalf of a passenger on or off of a portion of a train that will be inaccessible to the passenger while the train is in operation.
G. Interacting with travelling public (on board a vehicle or within a transportation facility) ..……....	Employees who provide services to passengers on-board a train or bus, including collecting tickets or cash for fares, providing information, and other similar services. Including: 1. On-board food or beverage employees. 2. Functions on behalf of an owner/operator regulated under this subchapter that require regular interaction with travelling public within a transportation facility, such as ticket agents.

H. Complying with security programs or measures, including those required by Federal law ……..	1. Employees who serve as security coordinators designated in §§ 1582.103 and 1582.211 of this subchapter, as well as any designated alternates or secondary security coordinators. 2. Employees who— a. Conduct training and testing of employees when the training or testing is required by TSA's security regulations. b. Manage or direct implementation of security plan requirements.

26. Add appendix C to part 1582 to read as follows:

Appendix C to Part 1582—Reporting of Significant Physical Security Concerns

Category	Description
Breach, Attempted Intrusion, and/or Interference …….....	Unauthorized personnel attempting to or actually entering a restricted area or secure site relating to a transportation facility or conveyance owned, operated, or used by an owner/operator subject to this part. This includes individuals entering or attempting to enter by impersonation of authorized personnel (for example, police/security, janitor, vehicle owner/operator). Activity that could interfere with the ability of employees to perform duties to the extent that security is threatened.
Misrepresentation ……..……	Presenting false, or misusing, insignia, documents, and/or identification, to misrepresent one's affiliation with an owner/operator subject to this part to cover possible illicit activity that may pose a risk to transportation security.
Theft, Loss, and/or Diversion	Stealing or diverting identification media or badges, uniforms, vehicles, keys, tools capable of compromising track integrity, portable derails, technology, or classified or sensitive security information documents which are proprietary to the facility or conveyance owned, operated, or used by an owner/operator subject to this part.
Sabotage, Tampering, and/or Vandalism ……...	Damaging, manipulating, or defeating safety and security appliances in connection with a facility, infrastructure, conveyance, or routing mechanism, resulting in the compromised use or the temporary or permanent loss of use of the facility, infrastructure, conveyance or routing mechanism. Placing or attaching a foreign object to a rail car or transit vehicle(s).
Expressed or Implied Threat	Communicating a spoken or written threat to damage or compromise a facility/infrastructure/conveyance owned, operated, or used by an owner/operator subject to this part (for example, a bomb threat or active shooter).
Eliciting Information ……	Questioning that may pose a risk to transportation or national security, such as asking one or more employees of an owner/operator subject to this part about particular facets of a facility's conveyance's purpose, operations, or security procedures.
Testing or Probing of Security……	Deliberate interactions with employees of an owner/operator subject to this part or challenges to facilities or systems owned, operated, or used by an owner/operator subject to this part that reveal physical, personnel, or security capabilities or sensitive information.
Photography ……	Taking photographs or video of facilities, conveyances, or infrastructure owned, operated, or used by an owner/operator subject to this part in a manner that may pose a risk to transportation or national security. Examples include taking photographs or video of infrequently used access points, personnel performing security functions (for example, patrols, badge/vehicle checking), or security-related equipment (for example, perimeter fencing, security cameras).
Observation or Surveillance .	Demonstrating unusual interest in facilities or loitering near conveyances, railcar routing appliances or any potentially critical infrastructure owned or operated by an owner/operator subject to this part in a manner that may pose a risk to transportation or national security. Examples include observation through binoculars, taking notes, or attempting to measure distances.
Materials Acquisition and/or Storage ……	Acquisition and/or storage by an employee of an owner/operator subject to this part of materials such as cell phones, pagers, fuel, chemicals, toxic materials, and/or timers that may pose a risk to transportation or national security (for example, storage of chemicals not needed by an employee for the performance of his or her job duties).

Category	Description
Weapons Discovery, Discharge, or Seizure…….	Weapons or explosives in or around a facility, conveyance, or infrastructure of an owner/operator subject to this part that may present a risk to transportation or national security (for example, discovery of weapons inconsistent with the type or quantity traditionally used by company security personnel).
Suspicious Items or Activity	Discovery or observation of suspicious items, activity or behavior in or around a facility, conveyance, or infrastructure of an owner/operator subject to this part that results in the disruption or termination of operations (for example, halting the operation of a conveyance while law enforcement personnel investigate a suspicious bag, briefcase, or package).

PART 1584—HIGHWAY AND MOTOR CARRIER SECURITY

27. Revise the authority citation for part 1584 to read as follows:

Authority: 49 U.S.C. 114; Pub. L. 110-53, 121 Stat. 266.

28. Revise subpart B of part 1584 to read as follows:

Subpart B—Security Programs: General

1584.101 Applicability.
1584.103 Physical Security Coordinator.
1584.105 Reporting of significant physical security concerns.
1584.107 Reporting cybersecurity incidents.
1584.109 [Reserved]
1584.111 [Reserved]
1584.113 Security training program requirements.
1584.115 [Reserved]

§ 1584.101 Applicability.

The requirements of this subpart apply to each OTRB owner/operator providing fixed-route service that originates, travels through, or ends in a geographic location identified in appendix A to this part.

§ 1584.103 Physical Security Coordinator.

(a) Each owner/operator identified in § 1584.101 must designate and use a primary and at least one alternate Physical Security Coordinator at the corporate level to function as the administrator for sharing security-related activities and information.

(b) The Physical Security Coordinator and alternate(s) must—

(1) Be accessible to TSA on a 24 hours per day, seven days per week basis;

(2) Serve as the primary contact(s) for intelligence information and security-related activities and communications with TSA. Any individual designated as a Physical

Security Coordinator may perform other duties in addition to the duties described in this section); and

(3) Coordinate security practices and procedures required by this subchapter internally and with appropriate law enforcement and emergency response agencies.

(c) The Physical Security Coordinator and alternate(s) must be a U.S. citizen eligible for a security clearance, unless otherwise waived by TSA.

(d) Each owner/operator required to have a Physical Security Coordinator must provide in writing to TSA the names, U.S. citizenship status, titles, business phone number(s), and business email address(es) of the Physical Security Coordinator and alternate Physical Security Coordinator(s). Changes in any of the information required by this section must be submitted to TSA within seven calendar days.

§ 1584.105 Reporting of significant physical security concerns.

(a) Each owner/operator identified in § 1584.101 must report, within 24 hours of initial discovery, any potential threats and significant physical security concerns involving transportation-related operations in the United States or transportation to, from, or within the United States as soon as possible by the methods prescribed by TSA.

(b) Potential threats or significant physical security concerns encompass incidents, suspicious activities, and threat information including, but not limited to, the categories of reportable events listed in appendix C to this part.

(c) Information reported must include the following, as available and applicable:

(1) The name of the reporting individual and contact information, including a telephone number or email address.

(2) The affected conveyance, station, terminal, or other transportation facility or infrastructure, including identifying information and current location.

(3) Scheduled origination and termination locations for the affected bus – including departure and destination station, city, and route, as applicable.

(4) Description of the threat, incident, or activity, including who has been notified and what action has been taken.

(5) The names, other available biographical data, and/or descriptions (including vehicle or license plate information) of individuals or motor vehicles known or suspected to be involved in the threat, incident, or activity.

(6) The source of any threat information.

§ 1584.107 Reporting cybersecurity incidents.

(a) *Reporting Cybersecurity Incidents*. Unless otherwise directed by TSA, each owner /operator identified in § 1584.101 must notify CISA of any Reportable Cybersecurity Incidents, as defined in the TSA Cybersecurity Lexicon, as soon as practicable, but no later than 24 hours after a Reportable Cybersecurity Incident is identified.

(b) Reports required by this section must be made by the methods prescribed by TSA. All reported information will be protected in a manner appropriate for the sensitivity and criticality of the information.

(c) The report to CISA must include the following information, as available to the reporting owner/operator at the time of the report:

(1) The name of the reporting individual and contact information, including a telephone number and email address. The report must also explicitly specify that the information is being reported to satisfy the reporting requirements in Transportation Security Regulations.

(2) The affected conveyance, system(s) or facilities, including identifying information and location.

(3) Description of the threat, incident, or activity, to include:

(i) Earliest known date of compromise;

(ii) Date of detection;

(iii) Information about who has been notified and what action has been taken;

(iv) Any relevant information observed or collected by the owner/operator, such as malicious Internet Protocol addresses, malicious domains, malware hashes and/or samples, or the abuse of legitimate software or accounts; and

(v) Any known threat information, to include information about the source of the threat or cybersecurity incident, if available.

(4) A description of the incident's impact or potential impact on Information or Operational Technology systems and operations. This information must also include an assessment of actual or imminent adverse impacts to service operations, operational delays, and/or data theft that have or are likely to be incurred, as well as any other information that would be informative in understanding the impact or potential impact of the cybersecurity incident.

(5) A description of all responses that are planned or under consideration.

(6) Any additional information not specifically required by this section, but which is critical to an understanding of the threat and owner/operator's response to a reportable cybersecurity incident.

(d) If all the required information is not available at the time of reporting, owner/operators must submit an initial report within the specified timeframe and supplement as additional information becomes available.

§ 1584.109 [Reserved]

§ 1584.111 [Reserved]

§ 1584.113 Security training program requirements.

(a) *Applicability.* This section applies to each owner/operator identified in § 1584.101.

(b) *Training required for security-sensitive employees.* No owner/operator identified in paragraph (a) of this section may use a security-sensitive employee to

perform a function identified in Appendix B to this part, unless that individual has received training as part of a security training program approved by TSA or is under the direct supervision of an employee who has received the training required by this section as applicable to that security-sensitive function. Upon approval, this security training program becomes part of the owner/operator's TSA-approved security program.

(c) *Limits on use of untrained employees.* Notwithstanding paragraph (b) of this section, a security-sensitive employee may not perform a security-sensitive function for more than 60 calendar days without receiving security training.

(d) *General requirements.* Each owner/operator required to provide security training to its employees under this section must submit their security training program to TSA for approval in a form and manner prescribed by TSA. The security training program must include the following information:

(1) Name of owner/operator.

(2) Name, title, telephone number, and email address of the primary individual to be contacted with regard to review of the security training program.

(3) Number, by specific job function category identified in Appendix B to this part, of security-sensitive employees trained or to be trained.

(4) Implementation schedule that identifies a specific date by which the required initial and recurrent security training will be completed.

(5) Location where training program records will be maintained.

(6) Plan for ensuring supervision of untrained security-sensitive employees performing functions identified in Appendix B to this part.

(7) Plan for notifying employees of changes to security measures that could change information provided in previously provided training.

(8) Method(s) for evaluating the effectiveness of the security training program in each area required by paragraph (e) of this section.

(e) *General curriculum requirements.* The security training program submitted to TSA for approval must include a curriculum or lesson plan, including learning objectives and method of delivery (such as instructor-led or computer-based training) for each course used to meet the requirements in paragraph (f) of this section. TSA may request additional information regarding the curriculum during the review and approval process. If recurrent training under paragraph (j) of this section is not the same as initial training, a curriculum or lesson plan for the recurrent training will need to be submitted and approved by TSA.

(f) *Specific curriculum requirements.* (1) *Prepare.* Each owner/operator must ensure that each of its security-sensitive employees with position- or function-specific responsibilities under the owner/operator's security program have knowledge of how to fulfill those responsibilities in the event of a security threat, breach, or incident to ensure—

(i) Employees with responsibility for transportation security equipment and systems are aware of their responsibilities and can verify the equipment and systems are operating and properly maintained; and

(ii) Employees with other duties and responsibilities under the company's security plans and/or programs, including those required by Federal law, know their assignments and the steps or resources needed to fulfill them.

(2) *Observe.* Each owner/operator must ensure that each of its security-sensitive employees has knowledge of the observational skills necessary to recognize—

(i) Suspicious and/or dangerous items, such as substances, packages, or conditions (for example, characteristics of an Improvised Explosive Device and signs of equipment tampering or sabotage);

(ii) Combinations of actions and individual behaviors that appear suspicious and/or dangerous, inappropriate, inconsistent, or out of the ordinary for the employee's

work environment, which could indicate a threat to transportation security; and

(iii) How a terrorist or someone with malicious intent may attempt to gain sensitive information or take advantage of vulnerabilities.

(3) *Assess.* Each owner/operator must ensure that each of its security-sensitive employees has knowledge necessary to—

(i) Determine whether the item, individual, behavior, or situation requires a response as a potential terrorist threat based on the respective transportation environment; and

(ii) Identify appropriate responses based on observations and context.

(4) *Respond.* Each owner/operator must ensure that each of its security-sensitive employees has knowledge of how to—

(i) Appropriately report a security threat, including knowing how and when to report internally to other employees, supervisors, or management, and externally to Local, State, or Federal agencies according to the owner/operator's security procedures or other relevant plans;

(ii) Interact with the public and first responders at the scene of the threat or incident, including communication with passengers on evacuation and any specific procedures for individuals with disabilities and the elderly; and

(iii) Use any applicable self-defense devices or other protective equipment provided to employees by the owner/operator.

(g) *Relation to other training.* Training conducted by owner/operators to comply with other requirements or standards, such as training for communicating with emergency responders to arrange the evacuation of passengers, may be combined with, and used to satisfy, elements of the training requirements in this section.

(h) *Submission.* If commencing or modifying operations subject to these requirements after June 21, 2021, the training program must be submitted to TSA no later

than 90 calendar days before commencing new or modified operations.

(i) *Initial security training.* Each owner/operator must provide initial security training to security-sensitive employees, using the curriculum approved by TSA and in compliance with the following schedule.

(1) For security training programs submitted to TSA for approval after March 22, 2021, if the employee is employed to perform a security-sensitive function on the date TSA approves the program, then initial training must be provided no later than twelve months after the date that TSA approves the owner/operator's security training program.

(2) If performance of a security-sensitive job function is initiated after TSA approves the owner/operator's security training program, then initial training must be provided no later than 60 calendar days after the employee first performs the security-sensitive job function.

(3) If the security-sensitive job function is performed intermittently, then initial security training must be provided no later than the 60th calendar day of employment performing a security-sensitive function, aggregated over a consecutive 12-month period.

(j) *Recurrent security training.* (1) Except as provided in paragraph (j)(2) of this section, a security-sensitive employee required to receive training must receive the required training at least once every 3 years.

(2) If an owner/operator modifies a security program or security plan for which training is required, the owner/operator must ensure each security-sensitive employee with position- or function-specific responsibilities related to the revised plan or program changes receives training on the revisions within 90 days of implementation of the revised plan or program changes. All other employees must receive training that reflects the changes to the operating security requirements as part of their regularly scheduled recurrent training.

(3) The 3-year recurrent training cycle is based on the anniversary calendar month

of the employee's initial security training. If the owner/operator provides the recurrent security training in the month of, the month before, or the month after it is due, the employee is considered to have taken the training in the month it is due.

(k) *Recognition of prior training.* Previously provided security training may be credited towards satisfying the requirements of this section provided the owner/operator—

(1) Obtains a complete record of such training and validates the training meets requirements of this section as it relates to the function of the individual security-sensitive employee, and the training was provided within the schedule required for recurrent training; and

(2) Retains a record of such training in compliance with the requirements in paragraph (l).

(l) *Retention of security training records.* The owner/operator must retain records of initial and recurrent security training records for each individual required to receive security training under this section for no less than 5 years from the date of training that, at a minimum—

(1) Includes employee’s full name, job title or function, date of hire, and date of initial and recurrent security training; and

(2) Identifies the date, course name, course length, and list of topics addressed for the security training most recently provided in each of the areas required under paragraph (e) of this section.

(m) *Availability of records to employees.* The owner/operator must provide records of security training to current and former employees upon request and at no charge as necessary to provide proof of training.

(n) *Incorporation into security program.* Once approved by TSA, the security training program required by this section is part of the owner/operator’s TSA-approved

security program. The owner/operator must implement and maintain the security training program and comply with timeframes for implementation identified in the security training program. Any modifications or amendments to the program must be made as stipulated in § 1570.107 of this subchapter.

(o) *Situations requiring owner/operator to revise security training program* . The owner/operator must submit a request to amend its security program if, after approval, the owner/operator makes, or intends to make, permanent (to be in effect for 60 or more calendar days) or substantive changes to its security training curriculum, including changes to address:

(1) Determinations that the security training program is ineffective based on the approved method for evaluating effectiveness in the security training program approved by TSA; or

(2) Development of recurrent training material for purposes of meeting the requirements in paragraph (j) of this section or other alternative training materials not previously approved by TSA.

§ 1584.115 [Reserved]

29. Revise appendix B to part 1584 to read as follows:

Appendix B to Part 1584—Security-Sensitive Job Functions for Over-the-Road Buses

This table identifies security-sensitive job functions for owner/operators regulated under this part. All employees performing security-sensitive functions are "security-sensitive employees" for purposes of this rule and must be trained in accordance with this part.

Categories	Security-Sensitive Job Functions for Over-the-Road Buses
A. Operating a vehicle…….....	Employees who have a CDL and operate an OTRB.

B. Inspecting and maintaining vehicles	Employees who— 1. Perform activities related to the diagnosis, inspection, maintenance, adjustment, repair, or overhaul of electrical or mechanical equipment relating to vehicles, including functions performed by mechanics and automotive technicians. 2. Does not include cleaning or janitorial activities.
C. Inspecting or maintaining building or transportation infrastructure	Employees who— 1. Provide cleaning services to areas of facilities owned, operated, or controlled by an owner/operator regulated under this subchapter that are accessible to the general public or passengers. 2. Provide cleaning services to vehicles owned, operated, or controlled by an owner/operator regulated under this part (does not include vehicle maintenance). 3. Provide general building maintenance services to buildings owned, operated, or controlled by an owner/operator regulated under this part.
D. Controlling dispatch or movement of a vehicle	Employees who— 1. Dispatch, report, transport, receive or deliver orders pertaining to specific vehicles, coordination of transportation schedules, tracking of vehicles and equipment. 2. Manage day-to-day delivery of transportation services and the prevention of, response to, and redress of disruptions to these services. 3. Perform tasks requiring access to or knowledge of specific route information.
E. Providing security of the owner / operator's equipment and property.....	Employees who patrol and inspect property of an owner/operator regulated under this part to protect the property, personnel, passengers and/or cargo.
F. Loading or unloading cargo or baggage	Employees who load, or oversee loading of, property tendered by or on behalf of a passenger on or off of a portion of a bus that will be inaccessible to the passenger while the vehicle is in operation.
G. Interacting with travelling public (on board a vehicle or within a transportation facility).....	Employees who— 1. Provide services to passengers on-board a bus, including collecting tickets or cash for fares, providing information, and other similar services. 2. Includes food or beverage employees, tour guides, and functions on behalf of an owner/operator regulated under this part that require regular interaction with travelling public within a transportation facility, such as ticket agents.
H. Complying with security programs or measures, including those required by Federal law	1. Employees who serve as security coordinators designated in § 1584.103 of this subchapter, as well as any designated alternates or secondary security coordinators. 2. Employees who— a. Conduct training and testing of employees when the training or testing is required by TSA's security regulations. b. Manage or direct implementation of security plan requirements.

30. Add appendix C to part 1584 to read as follows:

Appendix C to Part 1584—Reporting of Significant Physical Security Concerns

Category	Description
Breach, Attempted Intrusion, and/or Interference	Unauthorized personnel attempting to or actually entering a restricted area or secure site relating to a transportation facility or conveyance owned, operated, or used by an owner/operator subject to this part. This includes individuals entering or attempting to enter by impersonation of authorized personnel (for example, police/security, janitor, vehicle owner/operator). Activity that could interfere with the ability of employees to perform duties to the extent that security is threatened.

Category	Description
Misrepresentation ……..……	Presenting false, or misusing, insignia, documents, and/or identification, to misrepresent one's affiliation with an owner/operator subject to this part to cover possible illicit activity that may pose a risk to transportation security.
Theft, Loss, and/or Diversion	Stealing or diverting identification media or badges, uniforms, vehicles, keys, tools capable of compromising operating systems, technology, or classified or sensitive security information documents which are proprietary to the facility or conveyance owned, operated, or used by an owner/operator subject to this part.
Sabotage, Tampering, and/or Vandalism ……	Damaging, manipulating, or defeating safety and security appliances in connection with a facility, infrastructure, conveyance, or routing mechanism, resulting in the compromised use or the temporary or permanent loss of use of the facility, infrastructure, conveyance or routing mechanism. Placing or attaching a foreign object to a conveyance.
Expressed or Implied Threat.	Communicating a spoken or written threat to damage or compromise a facility/infrastructure/conveyance owned, operated, or used by an owner/operator subject to this part (for example, a bomb threat or active shooter).
Eliciting Information ……	Questioning that may pose a risk to transportation or national security, such as asking one or more employees of an owner/operator subject to this part about particular facets of a facility's conveyance's purpose, operations, or security procedures.
Testing or Probing of Security.……...	Deliberate interactions with employees of an owner/operator subject to this part or challenges to facilities or systems owned, operated, or used by an owner/operator subject to this part that reveal physical, personnel, or security capabilities or sensitive information.
Photography ……	Taking photographs or video of facilities, conveyances, or infrastructure owned, operated, or used by an owner/operator subject to this part in a manner that may pose a risk to transportation or national security. Examples include taking photographs or video of infrequently used access points, personnel performing security functions (for example, patrols, badge/vehicle checking), or security-related equipment (for example, perimeter fencing, security cameras).
Observation or Surveillance	Demonstrating unusual interest in facilities or loitering near conveyances, railcar routing appliances or any potentially critical infrastructure owned or operated by an owner/operator subject to this part in a manner that may pose a risk to transportation or national security. Examples include observation through binoculars, taking notes, or attempting to measure distances.
Materials Acquisition and/or Storage ……	Acquisition and/or storage by an employee of an owner/operator subject to this part of materials such as cell phones, pagers, fuel, chemicals, toxic materials, and/or timers that may pose a risk to transportation or national security (for example, storage of chemicals not needed by an employee for the performance of his or her job duties).
Weapons Discovery, Discharge, or Seizure…….	Weapons or explosives in or around a facility, conveyance, or infrastructure of an owner/operator subject to this part that may present a risk to transportation or national security (for example, discovery of weapons inconsistent with the type or quantity traditionally used by company security personnel).
Suspicious Items or Activity ……..	Discovery or observation of suspicious items, activity or behavior in or around a facility, conveyance, or infrastructure of an owner/operator subject to this part that results in the disruption or termination of operations (for example, halting the operation of a conveyance while law enforcement personnel investigate a suspicious bag, briefcase, or package).

31. Add part 1586 to read as follows:

PART 1586—PIPELINE FACILITIES AND SYSTEMS SECURITY

Subpart A—General

Sec.

§ 1586.1 Scope.

§ 1586.3 Terms used in this part.

§ 1586.5 Harmonization of Federal regulation.

Subpart B—Security Programs: Physical Security

Sec.

§ 1586.101. Scope and Applicability.

§ 1586.103 Physical Security Coordinator.

§ 1586.105 Reporting of significant physical security concerns.

Subpart C—Cybersecurity Risk Management

Sec.

§ 1586.201 Scope and applicability.

§ 1586.203. Form, content, and availability of Cybersecurity Risk Management program.

§ 1586.205 Cybersecurity evaluation.

§ 1586.207 Cybersecurity Operational Implementation Plan.

§ 1586.209 Governance of the CRM program.

§ 1586.211 Cybersecurity Coordinator.

§ 1586.213 Identification of Critical Cyber Systems.

§ 1586.215 Supply chain risk management.

§ 1586.217 Protection of Critical Cyber Systems.

§ 1586.219 Cybersecurity training and knowledge.

§ 1586.221 Detection of cybersecurity incidents.

§ 1586.223 Capabilities to respond to a cybersecurity incident.

§ 1586.225 Reporting cybersecurity incidents.

§ 1586.227 Cybersecurity Incident Response Plan.

§ 1586.229 Cybersecurity Assessment Plan

§ 1586.231 Documentation to establish compliance.

Appendix A to Part 1586—Reporting of Significant Physical Security Concerns

Authority: 49 U.S.C. 114; Public Law 110-53, 121 Stat. 266.

Subpart A—General

§ 1586.1 Scope.

This part includes requirements for the following persons. Specific sections in this part provide detailed applicability and requirements.

(a) Each person that owns or operates a hazardous liquid pipeline or system that is regulated under 49 CFR part 195; operates a primary control room responsible for multiple systems; or has a contract with the Defense Logistics Agency to supply hazardous liquids.

(b) Each person that owns or operates a natural and other gas pipeline system that is regulated under 49 CFR part 192; operates a primary control room responsible for multiple systems; or provides natural gas service to service points.

(c) Each person that owns or operates a liquefied natural gas facility that is regulated under 49 CFR part 193.

§ 1586.3 Terms used in this part.

In addition to the terms in §§ 1500.3, 1500.5, and 1503.103 of this chapter, the following terms apply to this part.

Control Room means an operations center staffed by personnel charged with responsibility for remotely monitoring and controlling a pipeline facility.

High Consequence Area has the same meaning as "high-consequence area" as defined in 49 CFR 192.903 and 49 CFR 195.450, as applicable.

Industrial control system (ICS) means an information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems used to control geographically dispersed assets, as well as distributed control

systems and smaller control systems using programmable logic controllers to control localized processes.

Peak-shaving facility means a pipeline facility that stores liquefied natural gas to meet demand spikes.

§ 1586.5 Harmonization of Federal regulation.

TSA will coordinate activities under this part with the Federal Energy Regulatory Commission (FERC), and the Pipeline and Hazardous Materials Safety Administration (PHMSA) of the Department of Transportation with respect to regulation of pipeline systems and facilities that are also licensed or regulated by the FERC or PHMSA, to avoid conflicting requirements and minimize redundancy of compliance activities.

Subpart B—Security Programs: Physical Security

§ 1586.101. Scope and Applicability.

(a) *Scope.* This subpart includes requirements that are primarily intended to ensure the physical security of pipeline facilities and systems. Physical security encompasses the security of systems and facilities, as well as the persons in areas in or near to operations that could have their safety and security threatened by an attack on physical systems and assets. Owner/operators identified in § 1586.1 must review the applicability in each section in this subpart to determine if any of the requirements apply to their operations.

(b) *Applicability.* Except as provided in paragraph (c) of this section, this subpart includes requirements for each owner/operator that meets any of the following criteria:

(1) Owns or operates a hazardous liquid or carbon dioxide pipeline or system regulated under 49 CFR part 195 and meets any of the following criteria:

(i) Delivers hazardous liquids or carbon dioxide more than 50 million barrels in any of the 3 calendar years before [EFFECTIVE DATE OF FINAL RULE] or any single calendar year after [EFFECTIVE DATE OF FINAL RULE]; or

(ii) Has more than 200 segment miles of pipeline transporting hazardous liquid or carbon dioxide that could affect a High Consequence Area.

(2) Owns or operates a primary control room responsible for multiple hazardous liquid or carbon dioxide systems regulated under 49 CFR part 196 and the total annual combined delivery for these systems is greater than 50 million barrels in any of the 3 calendar years before [EFFECTIVE DATE OF FINAL RULE] or any single calendar year after [EFFECTIVE DATE OF FINAL RULE].

(3) Owns or operates a hazardous liquid or carbon dioxide pipeline or system regulated under 49 CFR part 195 that has a contract with the Defense Logistics Agency to supply hazardous liquids more than 70,000 barrels annually.

(4) Owns or operates a natural and other gas pipeline system that is regulated under 49 CFR part 192 and meets any of the following criteria:

(i) Delivered natural or other gas more than 275 million dekatherms annually in any of the 3 calendar years before [EFFECTIVE DATE OF FINAL RULE] or any single calendar year after [EFFECTIVE DATE OF FINAL RULE];

(ii) Delivered natural or other gas to 275,000 or more meters (or service points) annually in any of the 3 calendar years before [EFFECTIVE DATE OF FINAL RULE] or any single calendar year after [EFFECTIVE DATE OF FINAL RULE]; or

(iii) Transmits natural or other gas more than 200 segment miles through a High Consequence Area.

(5) Operates a primary control room responsible for multiple natural or other gas pipeline systems regulated under 49 CFR part 192 systems and the combined total annual delivery or transmission for these systems is greater than 275 million dekatherms, in any of the 3 calendar years before [EFFECTIVE DATE OF FINAL RULE] or any single calendar year after [EFFECTIVE DATE OF FINAL RULE].

(6) Owns or operates a natural or other gas pipeline system regulated under 49

CFR part 192 that provides natural gas service to 275,000 or more meters (or service points) annually in any of the 3 calendar years before [EFFECTIVE DATE OF FINAL RULE] or any single calendar year after [EFFECTIVE DATE OF FINAL RULE].

(7) Each person that owns or operates a liquefied natural gas facility that is regulated under 49 CFR part 193 and—

(i) Imported natural gas in any of the 3 calendar years before [EFFECTIVE DATE OF FINAL RULE] or any single calendar year after [EFFECTIVE DATE OF FINAL RULE]; or

(ii) Operates as a "peak-shaving facility."

(c) The requirements in this part do not apply to U.S. facilities specified in 33 CFR 105.105(a) that are regulated under 33 CFR part 105 or facilities specified in 33 CFR 106.105(a) that are regulated under 33 CFR part 106.

§ 1586.103 Physical Security Coordinator.

(a) Each owner/operator identified in § 1586.101(b) must designate and use a primary and at least one alternate Physical Security Coordinator at the corporate level to function as the administrator for sharing security-related activities and information.

(b) The Physical Security Coordinator and alternate(s) must—

(1) Be accessible to TSA on a 24 hours per day, 7 days per week basis;

(2) Serve as the primary contact(s) for intelligence information and security-related activities and communications with TSA. Any individual designated as a Physical Security Coordinator may perform other duties in addition to the duties described in this section); and

(3) Coordinate security practices and procedures required by this subchapter internally and with appropriate law enforcement and emergency response agencies.

(c) The Physical Security Coordinator and alternate(s) must be a U.S. citizen eligible for a security clearance, unless otherwise waived by TSA.

(d) Each owner/operator required to have a Physical Security Coordinator must provide in writing to TSA the names, U.S. citizenship status, titles, business phone number(s), and business email address(es) of the Physical Security Coordinator and alternate Physical Security Coordinator(s). Changes in any of the information required by this section must be submitted to TSA within 7 calendar days.

§ 1586.105 Reporting of significant physical security concerns.

(a) Each owner/operator identified in § 1586.101(b) must report, within 24 hours of initial discovery, any potential threats and significant physical security concerns involving transportation-related operations in the United States or transportation to, from, or within the United States as soon as possible by the methods prescribed by TSA.

(b) Potential threats or significant physical security concerns encompass incidents, suspicious activities, and threat information including, but not limited to, the categories of reportable events listed in appendix A to this part.

(c) Information reported must include the following, as available and applicable:

(1) The name of the reporting individual and contact information, including a telephone number or email address.

(2) The affected system or facility, including identifying information and current location.

(3) Description of the threat, incident, or activity, including who has been notified and what action has been taken.

(4) The names, other available biographical data, and/or descriptions (including vehicle or license plate information) of individuals or motor vehicles known or suspected to be involved in the threat, incident, or activity.

(5) The source of any threat information.

Subpart C—Cybersecurity Risk Management

§ 1586.201 Scope and applicability.

(a) *Scope.* This subpart includes requirements to ensure the cybersecurity of gas hazardous liquid, carbon monoxide, and liquefied natural gas pipelines, pipeline systems, and facilities to mitigate the risk of significant harm significant harm to transportation facilities, as well as persons in areas in or near pipeline facilities and systems, that could have their safety and security threatened as a result of the degradation, destruction, or malfunction of systems that control these systems and infrastructure. In addition, cybersecurity incidents could have significant, similar impacts on the supply chain, affecting the national and economic security of the United States.

(b) *Applicability.* Each owner/operator described in § 1586.101(b) must adopt and carry out a Cybersecurity Risk Management (CRM) program.

§ 1586.203. Form, content, and availability of Cybersecurity Risk Management program.

(a) *General content requirements*. The CRM program required by this subpart is a comprehensive program that includes the following components:

(1) A cybersecurity evaluation completed and updated as required by § 1586.205;

(2) A TSA-approved Cybersecurity Operational Implementation Plan (COIP) that meets the requirements in § 1586.207.

(3) A Cybersecurity Assessment Plan that meets the requirements in § 1586.229.

(b) *Subsidiaries.* If a single CRM program is developed and implemented for multiple business units within a single corporate entity, any documents used to comply or establish compliance with the requirements in this subpart must clearly identify and distinguish application of the requirements to each business unit.

§ 1586.205 Cybersecurity evaluation.

(a) *General.* Each owner/operator required to have a CRM program must complete an initial and recurrent cybersecurity evaluation sufficient to determine the owner/operator's current enterprise-wide cybersecurity profile of logical/virtual and

physical security controls when evaluated against the CRM program requirements in this subpart, using a form provided by TSA or other tools approved by TSA.

(b) *Timing.* The initial cybersecurity evaluation must be completed no later than [DATE 90 DAYS AFTER EFFECTIVE DATE OF FINAL RULE], but no more than one year before the date of submission of the owner/operators Cybersecurity Operational Implementation Plan required by § 1586.207. If commencing or modifying operations subject to these requirements after [EFFECTIVE DATE OF FINAL RULE], the initial cybersecurity evaluation must be submitted to TSA no later than 45 calendar days after commencing the new or modified operations triggering applicability.

(c) *Annual updates.* The evaluation required by paragraph (a) of this section must be updated annually, no later than one year from the anniversary date of the previously completed evaluation.

(d) *Notification.* The owner/operator must notify TSA within 7 days of completing the evaluation and annual updates required by this section. A copy of the evaluation must be provided to TSA upon request.

(e) *Sensitive Security Information.* This evaluation is a vulnerability assessment as defined in § 1500.3 of this chapter and must be protected as Sensitive Security Information under § 1520.5(b)(5) of this chapter.

§ 1586.207 Cybersecurity Operational Implementation Plan.

(a) *Requirement.* Each owner/operator required to have a CRM program under this part must adopt a COIP.

(b) *General Content.* The COIP must include the following corporate information:

(1) The name and corporate address of the owner/operator;

(2) Written attestation by the owner/operator's accountable executive that the COIP has been reviewed and approved by senior management; and

(3) Identification of specific operations that meet the applicability criteria.

(c) *Specific Content.* The COIP must detail the owner/operator's defense-in-depth plan, including physical and logical/virtual security controls, to comply with the requirements and security outcomes specified in the following sections:

(1) *Governance.* The requirements for governance of the CRM program in § 1586.209 and the designation of a Cybersecurity Coordinator under § 1586.211.

(2) *Identification of Critical Cyber Systems, Network Architecture, and Interdependencies.* The requirements to identify Critical Cyber Systems and network architecture in § 1586.213 and supply chain risk management in § 1586.215.

(3) *Procedures, policies, and capabilities to protect Critical Cyber Systems.* The requirements for protection of Critical Cyber Systems in § 1586.217 and training of cybersecurity-sensitive employees in § 1586.219.

(4) *Procedures, policies, and capabilities to detect cybersecurity incidents.* The requirements for detecting cybersecurity incidents in § 1586.221.

(5) *Procedures, policies, and capabilities to respond to, and recover from, cybersecurity incidents.* The requirements for responding to cybersecurity incidents in § 1586.223, reporting cybersecurity incidents in § 1586.225, and the Cybersecurity Incident Response Plan in § 1586.227.

(d) *Plan of Action and Milestones.* (1) To the extent an owner/operator does not meet every requirement and security outcome identified in paragraph (c)(1) through (c)(5) of this section, the COIP must include a plan of action and milestones (POAM).

(2) The POAM must include:

(i) Policies, procedures, measures, or capabilities that owner/operator will develop or obtain, as applicable, to ensure all requirements and security outcomes in this subpart are met;

(ii) Physical and logical/virtual security controls that the owner/operator will

implement to mitigate the risks associated with not fully complying with requirements or security outcomes in this subpart; and

(iii) A detailed timeframe for full compliance with all requirements and security outcomes in this subpart, not to exceed three years from the date of submission to TSA of the COIP required by this section.

(3) The POAM must be updated as necessary to address any deficiencies identified during the evaluation required by § 1586.205 or as a result of an assessment conducted under § 1586.229 that will not be immediately addressed through an update to the COIP.

(e) *Approval and implementation.* (1) *Submission deadlines.* The COIP must be made available to TSA, in a form and manner prescribed by TSA, no later than [DATE 180 DAYS AFTER EFFECTIVE DATE OF FINAL RULE]. If commencing or modifying operations subject to these requirements after [EFFECTIVE DATE OF FINAL RULE], the COIP must be made available to TSA no later than 45 calendar days before commencing new or modified operations.

(2) *Effective date.* After considering all relevant materials and any additional information required by TSA, TSA will notify the owner/operator's accountable executive of TSA's decision to approve the owner/operator's COIP. The COIP becomes effective 30 days after the owner/operator is notified whether its COIP is approved.

(3) *TSA-approved security program.* Once approved by TSA, the COIP, any appendices, and any policies or procedures incorporated by reference, are a TSA-approved security program, subject to the protections in part 1520 of this chapter and the procedures applicable to security programs in subpart B of part 1570 of this subchapter.

(f) *Status Report and Updates.* The CRM program must be reviewed and updated by the owner/operator within 60 days of the evaluations or assessments required by §§ 1586.205 or 1586.229, as necessary to address any identified vulnerabilities or

weaknesses in the procedures, policies, or capabilities identified in the CRM program.

(g) *Revisions.* Unless otherwise specified in this subpart, any substantive modifications or amendments to the COIP must be made in accordance with the procedures in § 1570.107 of this subchapter.

§ 1586.209 Governance of the CRM program.

(a) *Accountable Executive.* (1) No later than [DATE 30 DAYS FROM EFFECTIVE DATE OF FINAL RULE], the owner/operator must provide to TSA the names, titles, business telephone numbers, and business email addresses of the owner/operator's accountable executive and the primary individual to be contacted about the owner/operator's CRM program. If any of the information required by this paragraph changes, the owner/operator must provide the updated information to TSA within 7 days of the change.

(2) The accountable executive must be an individual who has the authority and knowledge necessary for the development, implementation, and managerial oversight of the TSA-approved CRM program, including cybersecurity administration, risk assessments, inspections and control procedures, and coordinating communications with the owner/operator's leadership and staff on implementation and sustainment of the CRM program. To the extent possible, the accountable executive should not be the Cybersecurity Coordinator or an individual responsible for management of Information or Operational Technology system or systems' administration.

(b) *COIP.* The COIP must also include:

(1) Identification of positions designated by the owner/operator to manage implementation of policies, procedures, and capabilities described in the COIP and coordinate improvements to the CRM program.

(2) Corporate-level identification of any authorized representatives, as defined in the TSA Cybersecurity Lexicon, who are responsible for any or all the CRM program or

cybersecurity measures identified in the CRM program, and written documentation (such as contractual agreements) clearly identifying the roles and responsibilities of the authorized representative under the CRM program.

(3) The information required by paragraph (a)(1) of this section.

(c) *Process.* Updating the COIP to align with information provided to TSA under this section does not require an amendment subject to the procedures in § 1570.107 of this subchapter.

§ 1586.211 Cybersecurity Coordinator.

(a) Each owner/operator identified in paragraphs § 1586.101(b) must designate employees at the corporate level to serve as the primary and at least one alternate Cybersecurity Coordinator with responsibility for sharing critical cybersecurity information.

(b) The Cybersecurity Coordinator and alternate(s) must—

(1) Serve as the primary contact for cyber-related intelligence information and cybersecurity-related activities and communications with TSA and the Cybersecurity and Infrastructure Security Agency (CISA);

(2) Have the following knowledge and skills, through current certifications or equivalent job experience:

(i) General cybersecurity guidance and best practices;

(ii) Relevant law and regulations pertaining to cybersecurity;

(iii) Handling of Sensitive Security Information and security-related communications; and

(iv) Current cybersecurity threats applicable to the owner/operator's operations and systems.

(3) Be accessible to TSA and CISA 24 hours per day, 7 days per week;

(4) Have a Homeland Security Information Network (HSIN) account or other

TSA-designated communication platform for information sharing relevant to the requirements in this subpart; and

(5) Work with appropriate law enforcement and emergency response agencies in addressing cybersecurity threats or responding to cybersecurity incidents.

(c) The Cybersecurity Coordinator and alternate(s) must be a U.S. citizen eligible for a security clearance, unless otherwise waived by TSA.

(d) Owner/operators must provide in writing to TSA the names, titles, business phone number(s), and business email address(es) of the Cybersecurity Coordinator and alternate Cybersecurity Coordinator(s) required by paragraph (a) of this section no later than [DATE 7 DAYS AFTER EFFECTIVE DATE OF FINAL RULE], or within seven days of the commencement of new operations, or change in any of the information required by this section that occur after [DATE 7 DAYS AFTER EFFECTIVE DATE OF FINAL RULE].

(e) In addition to providing the information to TSA as required by paragraph (d), any owner/operator required to have a CRM program under this part must also include the information required by paragraphs (d) of this section in the COIP. As the owner/operator must separately notify TSA of this information, and any changes to this information, updating the COIP to align with information provided to TSA under this section does not require an amendment subject to the procedures in § 1570.107 of this subchapter.

§ 1586.213 Identification of Critical Cyber Systems.

(a) *Identifying information.* The owner/operator must incorporate into its COIP a list of Critical Cyber Systems, as defined in the TSA Cybersecurity Lexicon, that provides, at a minimum, the following identifying information for each Critical Cyber System:

(1) Identifier (system name or commercial name); and

(2) System manufacturer/designer name.

(b) *Identification methodology.* The owner/operator must include a description of the methodology and information used to identify Critical Cyber Systems that, at a minimum, includes the following information as used to identify critical systems:

(1) Standards and factors, including system interdependencies with critical functions, used to identify Information Technology and Operational Technology systems that could be vulnerable to a cybersecurity incident;

(2) Sources and data, such as known threat information relevant to the system, that informed decisions regarding the likelihood of the system being subject to a cybersecurity incident;

(3) Potential operational impacts of a cybersecurity incident, including scenarios that identify potential supply chain impacts and how long critical operations and capabilities could be sustained with identified alternatives if a system is offline; and

(4) Sustainability and operational impacts if an Information or Operational Technology system not identified as a Critical Cyber System becomes unavailable due to a cybersecurity incident.

(c) *System information and network architecture.* For all Critical Cyber Systems, the owner/operator must provide the following information:

(1) Information and Operational Technology system interdependencies for Critical Cyber Systems;

(2) All external connections to Critical Cyber Systems;

(3) Zone boundaries for Critical Cyber Systems, including a description of how Information and Operational Technology systems are defined and organized into logical/virtual zones based on criticality, consequence, and operational necessity;

(4) Baseline of acceptable communications between Critical Cyber Systems and external connections or between Information and Operational Technology systems; and

(5) Operational needs that prevent or delay implementation of the requirements in this subpart, such as application of security patches and updates, encryption of communications traversing Information and Operational Technology systems, and multi-factor authentication.

(d) *Additional systems.* If notified by TSA, the owner/operator must include additional Critical Cyber Systems identified by TSA not previously identified by the owner/operator.

(e) *Changes in Critical Cyber Systems.* Any substantive changes to Critical Cyber Systems require an amendment to the Cybersecurity Operational Implementation Plan subject to the procedures in § 1570.107 of this subchapter.

§ 1586.215 Supply chain risk management.

The owner/operator must incorporate into its COIP policies, procedures, and capabilities to address supply chain cybersecurity vulnerabilities that include requiring—

(a) All procurement documents and contracts, including service-level agreements, executed, or updated after [EFFECTIVE DATE OF FINAL RULE], include a requirement for the vendor or service provider to notify the owner/operator of the following:

(1) Cybersecurity incidents affecting the vendor or service provider within a specified timeframe sufficient for the owner/operator to identify and address any potential risks to their Critical Cyber Systems based on the scope and type of cybersecurity incident.

(2) Confirmed security vulnerabilities affecting the goods, services, or capabilities provided by the vendor or service provider within a specified timeframe sufficient for the owner/operator to identify and address any potential risks to their Critical Cyber Systems based on the scope and type of security vulnerability.

(b) Procurement documents and contracts, including service-level agreements,

incorporate an evaluation by the owner/operator or qualified third-party of the cybersecurity measures implemented by vendors or service providers of goods, services, or capabilities that will be connected to, installed on, or used by the owner/operator's Critical Cyber Systems.

(c) When provided two offerings of roughly similar cost and function, giving preference to the offering that provides the greater level of cybersecurity necessary to protect against, or effectively respond to, cybersecurity incidents affecting the owner/operator's Critical Cyber Systems.

(d) Upon notification of a cybersecurity incident or vulnerability under paragraphs (a) or (b) of this section, immediate consideration of mitigation measures sufficient to address the resulting risk to Critical Cyber Systems and, as applicable, revision to the COIP in accordance with § 1570.107 of this subchapter.

§ 1586.217 Protection of Critical Cyber Systems.

The owner/operator must incorporate into its COIP policies, procedures, controls, and capabilities to protect Critical Cyber Systems that meet security performance objectives in the following areas—

(a) *Network segmentation.* Network segmentation measures that protect against access to, or disruption of, the Operational Technology system if the Information Technology system is compromised or vice versa. These measures must be sufficient to—

(1) Ensure Information and Operational Technology system-services transit the other only when necessary for validated business or operational purposes;

(2) Secure and defend zone boundaries with security controls—

(i) To defend against unauthorized communications between zones; and

(ii) To prohibit Operational Technology system services from traversing the Information Technology system, and vice-versa, unless the content is encrypted at a level

sufficient to secure and protect integrity of data and prevent corruption or compromise while in transit. If encryption is not technologically feasible, ensure content is otherwise secured and protected using compensating controls that provide the same level of security as encryption for data in transit.

(b) *Access control.* Access control measures for Critical Cyber Systems, including for local and remote access, that secure and defend against unauthorized access to Critical Cyber Systems. These measures must, at a minimum, incorporate the following policies, procedures, and controls:

(1) Identification and authentication requirements designed to prevent unauthorized access to Critical Cyber Systems that include:

(i) A policy for memorized secret authenticator resets that includes criteria for passwords and when resets must occur, including procedures to ensure implementation of these requirements, such as password lockouts; and

(ii) Documented and defined logical/virtual and physical security controls for components of Critical Cyber Systems that will not be subject to the requirements in paragraph (b)(1)(i) of this section.

(2)(i) Except as provided in paragraph (b)(2)(ii), multi-factor authentication, or other logical/virtual and physical security controls to supplement memorized secret authenticators (such as passwords) to provide risk mitigation commensurate to multi-factor authentication.

(ii) An owner/operator in compliance with the requirements in 49 CFR 192.631 and 195.446, as applicable, may rely on the physical security measures as applied to the control room in lieu of applying multi-factor authentication to specific industrial control system workstations in the covered control room, as applicable, in lieu of implementing the requirements in paragraph (b)(2)(i). If relying on this exception, the owner/operator must identify the applicable system as a Critical Cyber System; maintain compliance with

the requirements in 49 CFR 192.631 and 195.446, as applicable; and include in the COIP a description of the physical security measures and other compensating controls used to prevent access to industrial control system workstations.

(3) Management of access rights based on the principles of least privilege and separation of duties. Where not technically feasible to apply these principles, the policies and procedures must describe compensating controls that the owner/operator applies.

(4) Policies and procedures limit availability and use of shared accounts to those that are critical for operations, and then only if necessary. When the owner/operator uses shared accounts for operational purposes, the policies and procedures must ensure:

(i) Access to shared accounts is limited through account management that uses principles of least privilege and separation of duties;

(ii) Any individual who no longer needs access does not have knowledge of the memorized secret authenticator necessary to access the shared account; and

(iii) Logs are maintained sufficient to enable positive user identification of access to shared accounts to enable forensic investigation following a cybersecurity incident.

(5) Regularly updated schedule for review of existing domain trust relationships to ensure their necessity and established and enforced policies to manage these relationships.

(c) *Patch management.* Measures that reduce the risk of exploitation of unpatched systems through the application of security patches and updates for operating systems, applications, drivers, and firmware on Critical Cyber Systems consistent with the owner/operator's risk-based methodology. These measures must include:

(1) A patch management strategy that ensures all critical security patches and updates on Critical Cyber Systems are current. This strategy must include:

(i) The risk methodology for categorizing and determining criticality of patches and updates, and an implementation timeline based on categorization and criticality; and

(ii) Prioritization of all security patches and updates on CISA's Known Exploited Vulnerabilities Catalog.

(2) In instances where the owner/operator cannot apply patches and updates on specific Operational Technology systems without causing a severe degradation of operational capability to meet business critical functions, the owner/operator must provide an explanation for why the actions cannot be taken and a description and timeline of additional mitigations that address the risk created by not installing the patch or update within the recommended timeframe.

(d) *Logging policies.* Logging policies sufficient to ensure logging data is—

(1) Stored in a secure and centralized system, such as a security information and event management tool or database on a segmented network that can only be accessed or modified by authorized and authenticated users; and

(2) Maintained for a duration sufficient to allow for investigation of cybersecurity incidents as supported by a risk analysis and applicable standards or regulatory guidelines.

(e) *Secure back-ups.* Policies that ensure all Critical Cyber Systems are backed-up on a regular basis consistent with operational need for the information, the back-ups are securely stored separate from the system, and policies require testing the integrity of back-ups to ensure that the data is free of known malicious code when the back-ups are made.

§ 1586.219 Cybersecurity training and knowledge.

(a) *Training required.* (1) Owner/operators required to have a CRM program under this subpart must provide basic cybersecurity training to all employees with access to the owner/operator's Information or Operational Technology systems.

(2) No owner/operator required to have a CRM program under this subpart may permit a cybersecurity-sensitive employee to access, or have privileges to access, a

Critical Cyber System or an Information or Operational Technology system that is interdependent with a Critical Cyber System, unless that individual has received basic and role-based cybersecurity training.

(b) *General curriculum requirements.* The cybersecurity training program must include a curriculum or lesson plan, including learning objectives and method of delivery (such as instructor-led or computer-based training) for each course used to meet the requirements in paragraphs (d) and (e) of this section. TSA may request additional information regarding the curriculum during the review and approval process. If recurrent training under paragraph (e) of this section is not the same as initial training, a curriculum or lesson plan for the recurrent training will need to be submitted and approved by TSA.

(c) *Specific curriculum requirements.* (1) *Basic cybersecurity training.* All employees and contractors with access to the owner/operator's Information or Operational Technology systems, must receive basic cybersecurity training that includes cybersecurity awareness to address best practices, acceptable use, risks associated with their level of privileged access, and awareness of security risks associated with their actions. This training must address the following topics:

(i) Social engineering, including phishing;

(ii) Password best practices;

(iii) Remote work security basics;

(iv) Safe internet and social media use;

(v) Mobile device (wireless) vulnerabilities and network security;

(vi) Data management and information security, including protecting business email, confidential information, trade secrets, and privacy; and

(vii) How and to whom to report suspected inappropriate or suspicious activity involving Information or Operational Technology systems, including mobile devices

provided by or connected to the owner/operator's Information or Operational Technology systems.

(2) *Role-based cybersecurity training.* Cybersecurity-sensitive employees must be provided cybersecurity training that specifically addresses their role as a privileged user to prevent and respond to a cybersecurity incident, acceptable uses, and the risks associated with their level of access and use as approved by the owner/operator. This training must address the following topics as applicable to the specific role:

(i) Security measures and requirements in the COIP including how the requirements affect account and access management, server and application management, and system architecture development and assessment;

(ii) Recognition and detection of cybersecurity threats, types of cybersecurity incidents, and techniques used to circumvent cybersecurity measures;

(iii) Incident handling, including procedures for reporting a cybersecurity incident to the Cybersecurity Coordinator and understanding their roles and responsibilities during a cybersecurity incident and implementation of the owner/operator's Cybersecurity Incident Response Plan required by § 1586.227;

(iv) Requirements and sources for staying aware of changing cybersecurity threats and countermeasures;

(v) Operational Technology-specific cybersecurity training for all personnel whose duties include access to Operational Technology systems.

(d) *Initial cybersecurity training.* (1) Each owner/operator must provide initial cybersecurity training (basic and role-based, as applicable) to employees and contractors, using the curriculum approved by TSA no later than 60 days after the effective date of the owner/operator's TSA-approved COIP required by this subpart.

(2) For individuals who onboard or become cybersecurity-sensitive employees after the effective date of the owner/operator's TSA-approved COIP who did not receive

training within the period identified in paragraph (d)(1) of this section, the individual must receive the applicable cybersecurity training no later than 10 days after onboarding.

(e) *Recurrent cybersecurity training.* Employees and contractors must receive annual recurrent cybersecurity training no later than the anniversary calendar month of the employee's initial cybersecurity training. If the owner/operator provides the recurrent cybersecurity training in the month of, the month before, or the month after it is due, the employee is considered to have taken the training in the month it is due.

(f) *Recognition of prior or established cybersecurity training.* Previously provided cybersecurity training may be credited towards satisfying the requirements of this section provided the owner/operator—

(1) Obtains a complete record of such training and validates the training meets requirements of this section as it relates to the role of the individual employee, and the training was provided within the schedule required for recurrent training; and

(2) Retains a record of such training in compliance with the requirements in paragraph (g) of this section.

(g) *Retention of cybersecurity training records.* The owner/operator must retain records of initial and recurrent cybersecurity training records for each individual required to receive cybersecurity training under this section for no less than 5 years from the date of training that, at a minimum—

(1) Includes employee's full name, job title or function, date of hire, and date of initial and recurrent cybersecurity training; and

(2) Identifies the date, course name, course length, and list of topics addressed for the cybersecurity training most recently provided in each of the areas required under paragraph (c) of this section.

(h) *Availability of records to employees.* The owner/operator must provide records of cybersecurity training to current and former employees upon request and at no

charge as necessary to provide proof of training.

§ 1586.221 Detection of cybersecurity incidents.

The owner/operator must incorporate into its COIP policies, procedures, and capabilities sufficient to detect and respond to cybersecurity threats to, and anomalies on, Critical Cyber Systems that, at a minimum—

(a) Defend against malicious email, such as spam and phishing emails, to preclude or mitigate against adverse impacts to operations;

(b) Block ingress and egress communications with known or suspected malicious Internet Protocol addresses;

(c) Control impact of known or suspected malicious web domains or web applications, such as by preventing users and devices from accessing malicious websites;

(d) Block and defend against unauthorized code, including macro scripts, from executing;

(e) Monitor and/or block connections from known or suspected malicious command and control servers (such as Tor exit nodes, and other anonymization services); and

(f) Ensure continuous collection and analysis of data for potential intrusions and anomalous behavior on Critical Cyber Systems and other Information and Operational Technology systems that directly connect with Critical Cyber Systems.

§ 1586.223 Capabilities to respond to a cybersecurity incident.

The owner/operator must incorporate into its COIP capabilities to respond to cybersecurity incidents affecting Critical Cyber Systems that, at a minimum—

(a) Audit unauthorized access to internet domains and addresses;

(b) Document and audit any communications between the Operational Technology system and an internal or external system that deviates from the owner/operator's identified baseline of communications;

(c) Identify and respond to execution of unauthorized code, including macro scripts; and

(d) Define, prioritize, and drive standardized incident response activities, such as Security Orchestration, Automation, and Response (SOAR).

§ 1586.225 Reporting cybersecurity incidents.

(a) Unless otherwise directed by TSA, each owner/operator identified in § 1586.101(b) must notify CISA of any Reportable Cybersecurity Incidents, as defined in the TSA Cybersecurity Lexicon, as soon as practicable, but no later than 24 hours after a Reportable Cybersecurity Incident is identified.

(b) Reports required by this section must be made by the methods prescribed by TSA. All reported information will be protected in a manner appropriate for the sensitivity and criticality of the information.

(c) The report to CISA must include the following information, as available to the reporting owner/operator at the time of the report:

(1) The name of the reporting individual and contact information, including a telephone number and email address. The report must also explicitly specify that the information is being reported to satisfy the reporting requirements in Transportation Security Regulations.

(2) The affected pipeline system(s) or facilities, including identifying information and location.

(3) Description of the threat, incident, or activity, to include:

(i) Earliest known date of compromise;

(ii) Date of detection;

(iii) Information about who has been notified and what action has been taken;

(iv) Any relevant information observed or collected by the owner/operators, such as malicious Internet Protocol addresses, malicious domains, malware hashes and/or

samples, or the abuse of legitimate software or accounts; and

(v) Any known threat information, to include information about the source of the threat or cybersecurity incident, if available.

(4) A description of the incident's impact or potential impact on Information or Operational Technology systems and operations. This information must also include an assessment of actual or imminent adverse impacts to service operations, operational delays, and/or data theft that have or are likely to be incurred, as well as any other information that would be informative in understanding the impact or potential impact of the cybersecurity incident.

(5) A description of all responses that are planned or under consideration, to include, for example, a reversion to manual operations and control, if applicable.

(6) Any additional information not specifically required by this section, but which is critical to an understanding of the threat and owner/operator's response to a reportable cybersecurity incident.

(d) If all the required information is not available at the time of reporting, owner/operators must submit an initial report within the specified timeframe and supplement as additional information becomes available.

§ 1586.227 Cybersecurity Incident Response Plan.

(a) The owner/operator must incorporate into its COIP an up-to-date Cybersecurity Incident Response Plan (CIRP) for the owner/operator's Critical Cyber Systems to reduce the impacts of a cybersecurity incident that causes, or could cause, operational disruption or significant impacts on business-critical functions.

(b) The CIRP must provide specific measures sufficient to ensure the following objectives, as applicable:

(1) Promptly identifying, isolating, and segregating the infected systems from uninfected systems, networks, and devices using measures that prioritize:

(i) Limiting the spread of autonomous malware;

(ii) Denying continued access by a threat actor to systems;

(iii) Determining extent of compromise; and

(iv) Preserving evidence and data.

(2) Only data stored and secured as required by § 1586.217(e) is used to restore systems and that all stored backup data is scanned with host security software to ensure the data is free of malicious artifacts before being used for restoration.

(3) Established capability and governance for implementing mitigation measures or manual controls that ensure that the Operational Technology system can be isolated when a cybersecurity incident in the Information Technology system creates risk to the safety and reliability of the Operational Technology system.

(c) The CIRP must identify who (by position) is responsible for implementing the specific measures in the plan and any necessary resources needed to implement the measures.

(d) The owner/operator must conduct an exercise to test the effectiveness of the CIRP no less than annually. The exercise conducted under this paragraph must—

(1) Test at least two objectives of the owner/operator's CIRP required by paragraph (b) of this section, no less than annually; and

(2) Include the employees identified (by position) in paragraph (c) as active participants in the exercise.

(e) Within no more than 90 days after the date of the exercise required by paragraph (d), the owner/operator must update the CIRP as appropriate to address any issues identified during the exercise.

(f) The owner/operator must notify TSA within 15 days of any changes to the CIRP. As the owner/operator must separately notify TSA, updating the COIP to align with information provided to TSA under this section does not require an amendment

subject to the procedures in § 1570.107 of this subchapter.

§ 1586.229 Cybersecurity Assessment Plan.

(a) *Requirement for a Cybersecurity Assessment Plan.* No later than 90 days from TSA's approval of the owner/operator's COIP, the owner/operator must submit to TSA a Cybersecurity Assessment Plan (CAP) sufficient to—

(1) Proactively assess the effectiveness of all policies, procedures, measures, and capabilities in the owner/operator's TSA-approved COIP as applied to all Critical Cyber Systems; and

(2) Identify and resolve device, network, and/or system vulnerabilities associated with Critical Cyber Systems.

(b) *Contents of the CAP.* At a minimum, the CAP must describe in detail:

(1) The plan to assess the effectiveness of the owner/operator's TSA-approved COIP as all applied to all Critical Cyber Systems;

(2) Schedule and scope of an architectural design review within 12 months either before or after TSA's approval of the owner/operator's COIP, to be repeated at least once every 2 years thereafter. The architectural design review required by this paragraph must include verification and validation of network traffic, a system log review, and analysis to identify cybersecurity vulnerabilities related to network design, configuration, and interconnectivity to internal and external systems;

(3) Other assessment capabilities designed to identify vulnerabilities to Critical Cyber Systems based on evolving threat information and adversarial capabilities, such as penetration testing of Information Technology systems, including the use of "red" and "purple" team (adversarial perspective) testing.

(c) *Specific Schedule.* (1) In addition to specifying the schedule for the architectural design review required by paragraph (b)(2), the CAP must include a schedule for conducting the assessments required by paragraph (b) sufficient to ensure at

least one-third of the policies, procedures, measures, and capabilities in the TSA-approved COIP are assessed each year, with 100 percent of the COIP and all Critical Cyber Systems assessed over a 3-year period.

(2) The scheduled required by this paragraph must map the planned assessments to the COIP and Critical Cyber System to document the plan will ensure all policies, procedures, measures, and capabilities in the owner/operator's TSA-approved COIP and all Critical Cyber Systems will be assessed within the timeframes required by paragraph (c)(1).

F(d) *Independence of assessors and auditors.* Owner/operators must ensure that the assessments, audits, testing, and other capabilities to assess the effectiveness of its TSA-approved COIP are not conducted by individuals who have oversight or responsibility for implementing the owner/operator's F program and have no vested or other financial interest in the results of the CAP.

(e) *Annual submission of report.* The owner/operator must ensure a report of the results of assessments conducted in accordance with the CAP is provided to corporate leadership and individuals designated under § 1586.209(a) and (b)(1), and submitted to TSA, no later than 15 months from the date of approval of the initial CAP and annually thereafter. The required report must indicate—

(1) Which assessment method(s) were used to determine if the policies, procedures, and capabilities described by the owner/operator in its COIP are effective; and

(2) Results of the individual assessment methodologies.

(f) *Annual update of the CAP.* The owner/operator must review and annually update the CAP to address any changes to policies, procedures, measures, or capabilities in the COIP or assessment capabilities required by paragraph (b). The updated CAP must be submitted to TSA for approval no later than 12 months from the date of TSA's

approval of the current CAP.

(g) Assessments conducted under this section are vulnerability assessments as defined in § 1500.3 of this chapter and must be protected as Sensitive Security Information under § 1520.5(b)(5) of this chapter.

§ 1586.231 Documentation to establish compliance.

For the purposes of the requirements in this subpart, upon TSA's request, the owner/operator must provide for inspection or copying the following types of information to establish compliance:

(a) Hardware/software asset inventory, including supervisory control and data acquisition (SCADA) systems;

(b) Firewall rules;

(c) Network diagrams, switch and router configurations, architecture diagrams, publicly routable internet protocol addresses, and Virtual Local Area Networks;

(d) Policy, procedural, and other documents that informed the development, and documented implementation of, the owner/operator's CRM program;

(e) Data providing a "snapshot" of activity on and between Information and Operational Technology systems such as:

(1) Log files;

(2) A capture of network traffic (such as packet capture (PCAP)), for a scope and period directed by TSA, not less than 24 hours and not to exceed 48 hours;

(3) "East-West Traffic" of Information Technology systems, sites, and environments within the scope of this subpart; and

(4) "North-South Traffic" between Information and Operational Technology systems, and the perimeter boundaries between them; and

(f) Any other records or documents necessary to determine compliance with this subpart.

Appendix A to Part 1586—Reporting of Significant Physical Security Concerns

Category	Description
Breach, Attempted Intrusion, and/or Interference …….....…	Unauthorized personnel attempting to or actually entering a restricted area or secure site relating to a pipeline facility or pipeline system owned, operated, or used by an owner/operator subject to this part. This includes individuals entering or attempting to enter by impersonation of authorized personnel (for example, police/security, janitor, vehicle owner/operator). Activity that could interfere with the ability of employees to perform duties to the extent that security is threatened.
Misrepresentation ……..……	Presenting false, or misusing, insignia, documents, and/or identification, to misrepresent one's affiliation with an owner/operator subject to this part to cover possible illicit activity that may pose a risk to transportation security.
Theft, Loss, and/or Diversion	Stealing or diverting identification media or badges, uniforms, vehicles, keys, tools capable of compromising operating systems, technology, or classified or sensitive security information documents which are proprietary to the pipeline facility or system owned, operated, or used by an owner/operator subject to this part.
Sabotage, Tampering, and/or Vandalism ……	Damaging, manipulating, or defeating safety and security appliances in connection with a pipeline facility, infrastructure, or systems resulting in the compromised use or the temporary or permanent loss of use of the pipeline facility, infrastructure, or system.
Expressed or Implied Threat	Communicating a spoken or written threat to damage or compromise a pipeline facility/infrastructure/system owned, operated, or used by an owner/operator subject to this part (for example, a bomb threat or active shooter).
Eliciting Information ……	Questioning that may pose a risk to transportation or national security, such as asking one or more employees of an owner/operator subject to this part about particular facets of a facility's or system's purpose, operations, or security procedures.
Testing or Probing of Security.……..….	Deliberate interactions with employees of an owner/operator subject to this part or challenges to pipeline facilities or systems owned, operated, or used by an owner/operator subject to this part that reveal physical, personnel, or security capabilities or sensitive information.
Photography ……	Taking photographs or video of pipeline facilities, systems, or infrastructure owned, operated, or used by an owner/operator subject to this part in a manner that may pose a risk to transportation or national security. Examples include taking photographs or video of infrequently used access points, personnel performing security functions (for example, patrols, badge/vehicle checking), or security-related equipment (for example, perimeter fencing, security cameras).
Observation or Surveillance	Demonstrating unusual interest in pipeline facilities or systems or loitering near facilities or systems or other potentially critical infrastructure owned or operated by an owner/operator subject to this part in a manner that may pose a risk to transportation or national security. Examples include observation through binoculars, taking notes, or attempting to measure distances.
Materials Acquisition and/or Storage ……	Acquisition and/or storage by an employee of an owner/operator subject to this part of materials such as cell phones, pagers, fuel, chemicals, toxic materials, and/or timers that may pose a risk to transportation or national security (for example, storage of chemicals not needed by an employee for the performance of his or her job duties).
Weapons Discovery, Discharge, or Seizure…….	Weapons or explosives in or around a pipeline facility, system, or infrastructure of an owner/operator subject to this part that may present a risk to transportation or national security (for example, discovery of weapons inconsistent with the type or quantity traditionally used by company security personnel).
Suspicious Items or Activity	Discovery or observation of suspicious items, activity or behavior in or around a pipeline facility, system, or infrastructure of an owner/operator subject to this part that results in the disruption or termination of operations (for example, halting operations while law enforcement personnel investigate a suspicious item, bag, package, etc.).

Dated: October 20, 2024.

David P. Pekoske,

Administrator.

[FR Doc. 2024-24704 Filed: 11/6/2024 8:45 am; Publication Date: 11/7/2024]