Enhancing Surface Cyber Risk Management

49 CFR Parts 1500, 1580, 1582, 1584, 1586

Docket No. TSA-2022-0001

RIN 1652-AA74

Notice of Proposed Rulemaking

Preliminary Regulatory Impact Analysis and Initial Regulatory Flexibility Analysis

September 2024

Economic Analysis Branch
Policy, Plans, and Engagement
Transportation Security Administration
Department of Homeland Security
Springfield, VA 22150

Table of Contents

Table of Figures

List of Abbreviations

9/11 Act	Implementing Recommendations of the 9/11 Commission Act of 2007
ABC	Anti-Bot Code of Conduct
ANPRM	Advance Notice of Proposed Rulemaking
ADR	Architectural Design Review
APTA	American Public Transportation Association
BLS	Bureau of Labor Statistics
CAGR	Compound Annual Growth Rate
CAP	Cybersecurity Assessment Plan
CFR	Code of Federal Regulations
CIP	Cybersecurity Implementation Plan
CIRP	Cybersecurity Incident Response Plan
CISA	Cybersecurity and Infrastructure Security Agency
COIP	Cybersecurity Operational Implementation Plan
COM	Cybersecurity Operations Manager
CPG	Cross-Sector Cybersecurity Performance Goals
CRM	Enhancing Surface Cyber Risk Management Notice of Proposed Rulemaking
CSE	Cybersecurity Evaluation
CSRIC	Communications Security Reliability, and Interoperability Council
DDoS	Distributed Denial-of-Service
DHS	U.S. Department of Homeland Security
DLA	Defense Logistics Agency
ECEC	Employer Cost of Employee Compensation
EO	Executive Order
FERC	Federal Energy Regulatory Commission
FRA	Federal Railroad Administration
FTP	File Transfer Protocol
GSA	General Services Administration
HCA	High Consequence Area
HSIN	Homeland Security Information Network
HTUA	High-Threat Urban Area
IC	Information Circular
ICS	Industrial Control Systems
IRFA	Initial Regulatory Flexibility Analysis
IT	Information Technology
LDC	Local Distribution Company

LNG	Liquefied Natural Gas
MFA	Multi-Factor Authentication
NAICS	North American Industry Classification System
NTD	National Transit Database
NIST	National Institute of Standards and Technology
NPRM	Notice of Proposed Rulemaking
OEWS	Occupational Employment and Wage Statistics
OMB	Office of Management and Budget
OT	Operational Technology
OTRB	Over-the-Road Bus
PRA	Paperwork Reduction Act of 1995
PHMSA	Pipeline and Hazardous Materials Safety Administration
POAM	Plan of Action and Milestones
PTC	Positive Train Control
PTPR	Public Transportation and Passenger Railroad
RIN	Regulation Identifier Number
RFA	Regulatory Flexibility Act of 1980, as amended
RIA	Regulatory Impact Analysis
SBA	Small Business Administration
SCADA	Supervisory Control and Data Acquisition
SD	Security Directive
SME	Subject Matter Expert
SOC	Standard Occupational Code
STA	Security Threat Assessment
STB	Surface Transportation Board
SVR	Foreign Intelligence Service of the Russian Federation
TB	Terabyte(s)
TPV	Third-Party Vendors
TSA	Transportation Security Administration
TSSRA	Transportation Sector Security Risk Assessment, Fiscal Year 2015 Report to Congress
UMRA	Unfunded Mandates Reform Act of 1995
U.S.C.	U.S. Code
VSL	Value of a Statistical Life

EXECUTIVE SUMMARY

Federal regulations must undergo several types of analyses, as required by Executive Orders (EOs), Acts, or Statutes, before their publication. EO 12866 directs agencies to assess the costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits.[1] Under EO 12866, as amended by EO 14094 (Modernizing Regulatory Review), the Office of Management and Budget (OMB) must determine whether a regulatory action is significant and therefore subject to the requirements of the EO.[2] EO 13563 emphasizes the importance of quantifying both costs and benefits, reducing costs, harmonizing rules, and promoting flexibility.

The TSA Enhancing Surface Cyber Risk Management (CRM) Notice of Proposed Rulemaking (NPRM), referred to as "the proposed rule" or the "CRM" rule throughout the rest of this document, is a "significant regulatory action" as defined in section 3(f) of EO 12866 and is economically significant as defined in section 3(f)(1) because its annual effect on the economy exceeds $200 million in at least one year of this Regulatory Impact Analysis (RIA).

The Regulatory Flexibility Act of 1980 (RFA), as amended by the Small Business Regulatory

[1] 58 FR 51735 (Oct. 4, 1993). https://www.reginfo.gov/public/jsp/Utilities/EO_12866.pdf. Accessed December 5, 2017.

[2] See section 1(b) of E.O. 14094, revising section 3(f) of EO 12866. Section 3(f) of EO 12866 defines a "significant regulatory action" as any regulatory action that is likely to result in a rule that: (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 affect 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) raise 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."

Enforcement Fairness Act of 1996, requires agencies to consider the economic impact of regulatory changes on small entities. The Trade Agreements Act of 1979 prohibits agencies from setting standards that create unnecessary obstacles to the foreign commerce of the United States. In developing U.S. standards, this act requires agencies to consider international standards and, where appropriate, to use them as the basis for U.S. standards. Finally, the Unfunded Mandates Reform Act of 1995 (UMRA) requires agencies to prepare a written assessment of the costs, benefits, and other effects of proposed or final rules 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 (adjusted for inflation) in any one year.

This RIA provides supporting documentation for the section *V. Regulatory Analyses* in the preamble of the NPRM for Enhancing Surface Cyber Risk Management (RIN 1652-AA74). TSA may not have precisely replicated the regulatory language of the NPRM in this RIA; and if finalized, the regulatory text, and not the text of this or any subsequent RIA, are legally binding. A summary of the RIA findings is presented below:

(1) This rulemaking is a significant regulatory action as defined under section 3(f)(1) of EO 12866 as amended by EO 14094 (Modernizing Regulatory Review), because the NPRM would result in an effect on the economy of $200 million or more in any year of the analysis;

(2) 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 28 of the small entities analyzed out of the 103 small entities that TSA found would be impacted by the NPRM;

(3) TSA has determined that the NPRM imposes no significant barriers to international trade as defined by the Trade Agreement Act of 1979; and

(4) Under Section 4 of UMRA, as codified at 2 U.S.C. 1503, 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.[3]

This proposed rule implements provisions in Parts 1570 (Maritime and Surface Transportation Security – General Rules), 1580 (Freight Rail Transportation Security), 1582 (Public Transportation and Passenger Railroad Security), 1584 (Highway and Motor Carrier Security), and 1586 (Pipeline Facilities and Systems Security) to address cybersecurity risks to transportation security under the authorities provided to the agency in the Aviation and Transportation Security Act (ATSA) and Implementing Recommendations of the 9/11 Commission Act (9/11 Act).

The proposed rule would be applicable to approximately 73 freight railroads of the 620 freight railroads operating in the United States, including the 6 Class I railroads, which account for

[3] *See* National Cybersecurity Strategy (March 2023) at 4 ("The cyber operations of criminal syndicates now represent a threat to the national security, public safety, and economic prosperity of the United States and its allies and partners. Ransomware incidents have disrupted critical services and businesses across the country and around the world, from energy pipelines and food companies, to schools and hospitals. Total economic losses from ransomware incidents continue to climb, reaching billions of U.S. dollars annually. Criminal syndicates often operate out of states that do not cooperate with U.S. law enforcement and frequently encourage, harbor, or tolerate such activities. These and other malicious cyber activities continue to threaten Americans across society, including disproportionately affecting those without the resources necessary to protect themselves, recover, or seek recourse."). This document is available at: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf. Accessed on July 20, 2023.

approximately 68 percent of freight rail mileage, 88 percent of employees, and 94 percent of revenue. It would also apply to 34 passenger railroads and transit rail systems of the 92 rail transit and passenger railroads operating in the United States and account for greater than 90 percent of nationwide daily passenger ridership.[4] In assessing the applicability factors for freight rail, the size (Class I/Short Line/Regional/Defense Connector) of the railroad was taken into account along with the volume of freight transported (400,000 train miles). The railroads in the applicability pool represent the major carriers across the Nation without including smaller operators that only have a limited impact to the national rail system. When developing the criteria for PTPR, TSA considered daily ridership as the key risk consideration, as higher ridership represents larger potential consequence.[5] The rule would also be applicable to 71 over-the-road buses (OTRB) owner/operators who are currently subject to TSA's regulatory requirements to report security incidents. Finally, TSA estimates the rule would also apply to 115 hazardous liquid pipelines and natural gas and other gas pipelines of which 66 are natural gas, 39 are hazardous liquids, 9 are Liquefied Natural Gas (LNG), and 1 is chemical and account for approximately 91 percent of the total annual volume transported in the United States.

The proposed rule would require designated owner/operators for all four modes to report cybersecurity incidents to the Cybersecurity and Infrastructure Agency (CISA).[6] Designated owner/operators of freight railroads, PTPR, and pipeline facilities and systems would also be

---

[4] American Public Transportation Association (APTA). 2022 Public Transportation Fact Book. https://www.apta.com/research-technical-resources/transit-statistics/public-transportation-fact-book/. Accessed on June 27, 2023. For purposes of this analysis, PTPR is comprised of 92 Transit Rail and Passenger Railroad systems made up of 30 Commuter Rail, 15 Heavy Rail, 23 Light Rail, and 24 Streetcar.

[5] TSA also considered 49 CFR 1582; Appendix A, where TSA has previously defined high-risk entities for training requirements.

[6] TSA notes if CISA issues a final rule regarding reporting of cybersecurity incidents before TSA finalizes this proposed rule, TSA will review that rule to avoid unnecessary duplication of reporting requirements that could result in additional costs.

required to identify a cybersecurity coordinator, and develop and implement a comprehensive CRM program. The proposed CRM program includes three primary elements. First, owner/operators would be required to regularly conduct an enterprise-wide cybersecurity evaluation that would identify the current profile of cybersecurity. Second, owner/operators would be required to develop a Cybersecurity Operational Implementation Plan (COIP) with requirements that focus on: (a) governance of the CRM program, (b) identification of Critical Cyber Systems; (c) protecting Critical Cyber Systems; (d) detecting and monitoring Critical Cyber Systems; and (e) ensuring response and recovery. As part of the COIP process to ensure response and recovery, owner/operators would develop a Cybersecurity Incident Response Plan (CIRP) that requires an established set of policies and procedures in place to respond to intrusions into their critical cybersecurity systems as well as maintenance or reconstitution of operations during an incident which has been evaluated separately in this RIA. Third, owner/operators would be required to have a Cybersecurity Assessment Plan (CAP) that includes an independent evaluation of the effectiveness of their CRM program and identification of unaddressed vulnerabilities. The rule would also expand the requirement for having a physical security coordinator (currently in 49 CFR 1570.201) and reporting physical security incidents (currently in 49 CFR 1570.203) to owner/operators of designated pipeline facilities and systems.

Need for Regulatory Action

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 counterterrorism mission assigned to TSA. 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.[7]

Transportation companies are managing competing priorities with finite resources. With the uncertainty surrounding future technological innovation and the corresponding threat evolution, there is an additional layer of complexity added to the analysis of building a cybersecurity defense. Given the ever-present threat of cybersecurity attacks and the potential economic and societal consequences, TSA believes there is a need for this regulation.

A successful attack could result in real world negative consequences. For example, a successful cyber-intrusion affecting Operational Technology (OT) systems could impact industrial control systems (ICS) including Supervisory Control and Data Acquisition (SCADA) systems, process control systems, distributed control systems, measurement systems, and telemetry systems which could impact the ability for companies to safely operate their systems. In December 2020, a highly sophisticated attack was discovered targeting SolarWinds, an Information Technology (IT) management software provider. The compromised SolarWinds software led to the distribution of a malware-infected update to their Orion platform.[8] This attack impacted numerous organizations and government agencies, including the U.S. Department of Defense and the Department of Homeland Security (DHS). As the Cybersecurity and Infrastructure Security Agency (CISA) has noted, recent cybersecurity incidents demonstrate that intrusions

---

[7] Surface Transportation and Rail Security Act of 2007, report of the Senate Committee on Commerce, Science, and Transportation at 2 (S Rpt. 110-29, dated March 1, 2007) quoting EO 13416 (Dec. 5, 2006), published at 71 FR 71033 (Dec. 7, 2006). https://www.govinfo.gov/content/pkg/CRPT-110srpt29/html/CRPT-110srpt29.htm.

[8] See Martínez, J., & Durán, J. N. (2021). Software Supply Chain Attacks, a Threat to Global Cybersecurity: SolarWinds' Case Study. International Journal of Safety and Security Engineering, 11(5), 537–545. https://doi.org/10.18280/ijsse.110505 and Peisert, S., Schneier, B., Okhravi, H., Massacci, F., Benzel, T., Landwehr, C. E., Mannan, M., Mirkovic, J., Prakash, A., & Michael, J. B. (2021). Perspectives on the SolarWinds Incident. IEEE Security & Privacy, 19(2), 7–13. https://doi.org/10.1109/msec.2021.3051235

affecting IT systems can also affect critical operational processes even if the intrusion does not directly impact OT systems.[9]

The cyber threat to the country's critical infrastructure has likely continued to increase in the time since the initial security directives addressing cybersecurity in surface transportation were issued 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.[10]

Therefore, TSA is proposing regulatory action to develop a CRM system requiring regulated parties to appoint a cybersecurity coordinator, report cybersecurity incidents, and develop a comprehensive cybersecurity risk management program thereby addressing the threat posed by cyber-attacks and inconsistent levels of cybersecurity protection across industry. By structuring the requirements from a performance focus, rather than prescriptive requirements, covered owner/operators would maintain the flexibilities needed to account for differences in business operations while still establishing benchmark and uniform guidelines to ensure increased cybersecurity across the full industries. Transportation companies can help protect critical infrastructure, maintain economic stability, and ensure the safe and reliable movement of goods and people by implementing new cybersecurity requirements and adopting robust security measures.

---

[9] *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.

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

Baseline Summary

This section presents a brief description of each impacted industry and baseline cybersecurity measures currently in place for each of the modes of surface transportation. The baseline represents TSA's best assessment of what the world would be like in the absence of regulatory action.[11]

In general, there are a number of cybersecurity standards available as a resource for owners/operators across industry. For example, the National Institute of Standards and Technology (NIST) provides an organizing framework to establish cybersecurity standards that details five pillars of focus: Identify, Protect, Detect, Respond, Recover.[12] Additionally, recommendations found in CISA's Cross-Sector Cybersecurity Performance Goals (CPGs) provide actions that could result in an outcome that reduces cybersecurity risk.[13] However, implementation of such standards are not required and it is up to individual companies to choose their level of adherence.

TSA also recently issued security directives (SD) in 2021, 2022, and 2023 in response to cybersecurity risks to designated freight railroads, passenger rail and rail transit owner/operators, and pipeline owner/operators whose specifics are provided below. 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 measures.[14] In

---

[11] Office of Information and Regulatory Affairs. "Regulatory Impact Analysis: A Primer." p. 4. August 15, 2011. https://www.reginfo.gov/public/jsp/Utilities/circular-a-4_regulatory-impact-analysis-a-primer.pdf. Accessed on Aug. 4, 2023.

[12] For more information, see the NIST Cybersecurity Framework at https://www.nist.gov/cyberframework.

[13] For more information, see CISA's CPGs at https://www.cisa.gov/cross-sector-cybersecurity-performance-goals

[14] *See* Information Circular: Surface Transportation IC-2021-01: Enhancing Surface Transportation Cybersecurity at https://www.tsa.gov/sites/default/files/20211201_surface-ic-2021-01.pdf. Accessed on Oct. 19, 2022. Information Circular applicability indicates freight rail, PTPR, and OTRB.

response to TSA's SDs, many affected owner/operators have taken action, incurred costs, and started to implement many of the cybersecurity risk management program elements that are required in the proposed rule.

However, given the recency of the SDs and voluntary nature of previous industry cybersecurity efforts with no specific requirements included in regulation, TSA uses a zero baseline that evaluates all rule requirements as new and thus provides an assessment of the impact of the full CRM program. Assuming a baseline level of compliance as zero ensures TSA captures all of the costs related to the requirements of this rulemaking.

TSA recognizes that some of the rule provisions may have already been implemented through current industry cybersecurity practices or in response to TSA's security directives (SDs) and thus a portion of the costs may have already been incurred. However, TSA doesn't specifically quantify the relative incremental impacts of the NPRM (e.g., since the issuance of the SDs); but does provide an accounting of costs for requirements captured by SDs and a sensitivity analysis that considers possible existing industry efforts on key cost drivers.

Freight Rail

The national freight rail network is a complex system that includes both physical and cyber infrastructure and consists of nearly 140,000 rail miles operated by six Class I railroads, 580 local (also known as Short Line) railroads, and 21 regional railroads. Freight railroads are private entities which own and are responsible for their own infrastructure. They maintain the locomotives, rolling stock, and fixed assets involved in the transportation of goods and materials across the Nation's rail system. TSA administers and enforces rail security regulations contained in 49 CFR part 1580.

TSA assumes many owner/operators have implemented a variety of cybersecurity protection and risk management measures; however, such implementation is voluntary and varies across the industry. Recently, TSA issued security directives (SD) to higher-risk freight railroads in response to cybersecurity risks. In December 2021, TSA's SD 1580-21-01 series requirements included: (1) designation of a cybersecurity coordinator and alternate; (2) reporting of cybersecurity incidents to CISA within 24 hours; (3) developing and implementing a CIRP to reduce the risk of an operational disruption; and (4) completing a cybersecurity vulnerability assessment to identify potential gaps or vulnerabilities in their systems.[15] In October of 2022, TSA issued a SD imposing performance-based cybersecurity requirements on higher-risk freight railroads and passenger rail owner/operators (SD 1580/82-2022-01).[16]

Public Transit Passenger Railroad (PTPR)

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 sole long-distance inter-city passenger railroad in the contiguous United States is Amtrak. While PTPR typically includes buses, for purposes of this proposed rulemaking, PTPR is limited to rail transit and passenger rail. Freight railroads provide the tracks for most passenger rail operations. For example, seventy-two percent of the track on which Amtrak operates is owned by other railroads. Amtrak and other passenger rail agencies, however, are not wholly dependent on freight rail infrastructure and corridors for operations; they sometimes control, operate, and maintain tracks, facilities, construction sites, utilities, and

[15] *See* SD 1580-21-01A: Enhancing Rail Security at https://www.tsa.gov/sites/default/files/sd-1580-21-01a.pdf Accessed on Oct. 19, 2022.
[16] *See* SD 1580/82-2022-01: Rail Cybersecurity Mitigation Actions and Testing at https://www.tsa.gov/sites/default/files/sd-1580-82-2022-01.pdf. Accessed on Oct. 19, 2022.

computerized networks essential to their own operations. Amtrak and other passenger railroads also host freight rail operations in some instances. TSA administers and enforces passenger rail security regulations contained in 49 CFR part 1582.

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. In major metropolitan areas, commuters rely on public transportation for their daily commute.[17] Rail transit is a critical part of the overall public transit system, representing about 52 percent of all passenger miles traveled on public transit.[18]

As with freight rail, TSA assumes many owner/operators have implemented a variety of cybersecurity protection and risk management measures but that such implementation is voluntary and varies across the industry. In addition, TSA also issued SDs to passenger rail and rail transit owner/operators. TSA's December 2021 SD 1582-21-01 series requirements included: (1) designation of a cybersecurity coordinator and alternate; (2) reporting of cybersecurity incidents to CISA within 24 hours; (3) developing and implementing a CIRP to reduce the risk of an operational disruption; and (4) completing a cybersecurity vulnerability assessment to identify potential gaps or vulnerabilities in their systems.[19] In October of 2022, TSA issued a SD imposing performance-based cybersecurity requirements on higher-risk freight railroads and

---

[17] *See* APTA, 2022 Public Transportation Fact Book at 12. Available at https://www.apta.com/research-technical-resources/transit-statistics/public-transportation-fact-book/

[18] 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.

[19] *See* SD 1582-21-01A: Enhancing Public Transportation and Passenger Railroad Cybersecurity at https://www.tsa.gov/sites/default/files/sd-1582-21-01a.pdf. Accessed on Oct. 19, 2022.

passenger rail owner/operators (SD 1580/82-2022-01).[20]

Highway Motor Carrier

According to the 2020 Motorcoach Census, 1,717 companies operated 27,753 motorcoaches in the United States, and nearly 125 million passenger trips were provided across the United States and Canada, in 2020.[21] The services provided by the over-the-road-bus (OTRB) providers are a necessary and important part of transportation for Americans. TSA estimates that 71 OTRB owner/operators fall within the applicability of the rule. Currently, it is recommended via an information circular (IC-2021-01) that cybersecurity incidents are reported to CISA. Although some OTRB operators may be voluntarily following the information circular guidance, TSA is assuming the proposed rule requirements as new and presents a baseline level of compliance of zero to capture the full regulatory impact of the rule.

Pipeline

The national pipeline system consists of more than 2.96 million miles of networked pipelines transporting hazardous liquids, natural gas, and other liquids and gases for energy needs and manufacturing.[22] They are monitored and moderated through automated ICS, such as SCADA systems. These systems use remote sensors, signals, and preprogramed parameters to activate valves and pumps to maintain flows within tolerances. Pipeline systems supply energy commodities and raw materials across the country to utility entities, airports, military sites, and to the Nation's industrial and manufacturing sectors. Vital components of the mode include

---

[20] *See* SD 1580/82-2022-01: Rail Cybersecurity Mitigation Actions and Testing at https://www.tsa.gov/sites/default/files/sd-1580-82-2022-01.pdf.Accessed on Oct. 19, 2022.

[21] See the American Bus Association, 2022 Motorcoach Census. Available at https://www.buses.org/assets/images/uploads/pdf/Motorcoach_Census_Survey_2020.pdf. Accessed June 9, 2023.

[22] Mileage is available via the Pipeline and Hazardous Materials Safety Administration at https://www.phmsa.dot.gov/data-and-statistics/pipeline/annual-report-mileage-summary-statistics. Accessed on November 30, 2023.

assets, components, and industrial automated, semi-automated, and manual control systems.

TSA assumes many pipeline owner/operators have implemented a variety of cybersecurity protection and risk management measures; but that implementation of such measures done beyond the requirements stated in the SDs are voluntary and vary across the industry. However, TSA finds pipelines are still at risk from cybersecurity threat. As part of the effort to mitigate this potential issue and the cybersecurity risk facing the industry, TSA issued SDs to higher-risk pipeline owner/operators. In May 2021, TSA issued SD-Pipeline-2021-01 which required certain pipeline owner/operators to: (1) designate a primary and alternate cybersecurity coordinator; (2) report cybersecurity incidents to CISA within 24 hours of identification of a cybersecurity incident; and (3) review TSA's pipeline guidelines, assess their current cybersecurity posture, and identify remediation measures to address the vulnerabilities and cybersecurity gaps. Then, in July 2021 TSA issued a second directive (SD-Pipeline-2021-02) which required owner/operators to implement specific mitigation measures to protect against ransomware incidents and other known threats to IT and OT systems and conduct a cybersecurity architecture design review. It also required owner/operators to develop and adopt a CIRP to reduce the risk of operational disruption should their IT and/or OT systems be affected by a cybersecurity incident.[23]

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 this, TSA revised this SD series, effective July 2022 (SD Pipeline-2021-02C), to maintain the security

[23] *See* SD Pipeline-2021-01B: Enhancing Pipeline Cybersecurity at https://www.tsa.gov/sites/default/files/sd_pipeline-2021-01b_05-29-2022.pdf for a version of the SD with the prescriptive requirements initially imposed. Accessed on Oct. 19, 2022.

objectives in the previous versions of the SD but also provide more flexibility by imposing performance-based, rather than prescriptive, security measures. This directive requires certain pipeline operators to do the following:

- Establish and implement a TSA-approved Cybersecurity Implementation Plan that describes the specific cybersecurity measures employed 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 significant impacts on necessary capacity, as defined in the SD, should the IT and/or OT systems of a gas or liquid pipeline be affected by a cybersecurity incident.
- Establish a Cybersecurity Assessment Program and submit an annual plan that describes how the owner/operator will proactively and regularly assess the effectiveness of cybersecurity measures and identify and resolve device, network, and/or system vulnerabilities.

Costs of the Proposed Rule

The purpose of this proposed rule is to strengthen cybersecurity measures and resiliency for the surface transportation sector by imposing requirements to report cybersecurity incidents and develop a robust CRM program for freight rail, PTPR, OTRB owner/operators, and pipeline owner/operators. For owner/operators of these modes and TSA, there are cybersecurity and physical security costs associated with compliance of the proposed rule. Table ES - 1 presents a breakdown of the costs industry and TSA would incur from implementing all of the requirements in the proposed rule. A detailed discussion of the assumptions used and the costs for this rulemaking can be found in Sections 2 and 3 of this RIA. As noted above, and further discussed in Section 1.7, TSA estimates the full costs of the CRM program without adjusting for costs

industry has incurred voluntarily or as a result of TSA SDs.[24] Consequently, the cost estimates below are likely an overestimate.

Table ES - 1: Total Ten-Year Costs of the Proposed Rule by Requirement (Discounted at 7 Percent, $ Thousands)

NPRM Requirements	49 CFR	Ten-Year Costs	Description
Cybersecurity Evaluation (CSE)	§ 1580.305 § 1582.205 § 1586.205	$9,830.5	Owner/operators are expected to evaluate and create a current profile of CRM program including both physical and logical/virtual security controls.
Cybersecurity Operational Implementation Plan (COIP)	§ 1580.307 § 1582.207 § 1586.207	Costs are captured under requirements below	Require owner/operators to detail their defense-in-depth plan, including physical and logical/virtual security controls, to comply with the requirements and how the owner/operator meets these requirements for governance, identification of critical systems, protection of critical systems, detection and response of incidents.
Governance of the CRM	§ 1580.309 § 1582.209 § 1586.209	$11,501.9	Each owner/operator must identify an Accountable Executive and keep this information updated with TSA. 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. The COIP must also include identification of positions designated to manage implementation of policies and procedures and any authorized representatives responsible for implementation and oversight of the CRM.
Cybersecurity Coordinator	§ 1580.311 § 1582.211 § 1586.211	$289.9	Owner/operators are required to designate a cybersecurity coordinator who is required to be available to TSA and DHS's Cybersecurity and Infrastructure Security Agency (CISA) at all times (all hours/all days) to coordinate cybersecurity and address any incidents that arise.
Identification of Critical Cyber Systems	§ 1580.313 § 1582.213 § 1586.213	$8,317.7	Owner/operators must identify Critical Cyber Systems including the identifying information, identification methodology, system information and network architecture, additional systems, and changes to Critical Cyber Systems.

[24] Section 3.7 provides a SD to rule comparison that further discusses the relationship between the proposed rule and SDs and their associated costs.

NPRM Requirements	49 CFR	Ten-Year Costs	Description
Supply chain risk management	§ 1580.315 § 1582.215 § 1586.215	$50,635.6	Owner/operators will consider cybersecurity in all aspects of vendor and procurement agreements. Owner/operators are encouraged to select the more secure offer between two vendors of similar cost and function. All procurement documents and contracts, including service-level agreements, executed or updated after the effective date of the final rule include a requirement for vendor or service providers to notify owner/operators of cyber incidents affecting vendor or service providers and confirmed security vulnerabilities affecting the vendor service. Upon notification of a cybersecurity event or vulnerability, owner/operators must consider mitigation measures sufficient to address the resulting risk to Critical Cyber Systems and, if any of these measures would result in permanent changes, the owner/operator would need to request to amend its COIP.
Protection of Critical Cyber Systems	§ 1580.317 § 1582.217 § 1586.217	$1,738,813.0	The owner/operator must incorporate into its COIP network segmentation and other policies, procedures, controls and capabilities to protect Critical Cyber Systems. This includes IT/OT communications, patching, ensuring logging data are secured and stored centrally, backups, and protections that control access to systems.
Cybersecurity training and knowledge	§ 1580.319 § 1582.219 § 1586.219	$215,981.0	Owner/operators required to have a CRM program must provide basic cybersecurity training to all employees, including contractors, with access to the owner/operator's Information or Operational Technology systems, and role-based cybersecurity training for cybersecurity-sensitive employees.
Detection of cybersecurity incidents	§ 1580.321 § 1582.221 § 1586.221	$15,548.1	The owner/operator must incorporate into its COIP policies, procedures, and capabilities sufficient to detect o cybersecurity threats to, and anomalies on, Critical Cyber Systems.
Capabilities to respond to a cybersecurity incident	§ 1580.323 § 1582.223 § 1586.223	Cost captured in Reporting and Detection of Cyber Incidents	The owner/operator must incorporate into its COIP capabilities to respond to cybersecurity incidents affecting Critical Cyber Systems, including documenting and auditing any communications between OT and IT systems, responding to execution of unauthorized code, and ensuring standardized incident response activities.
Reporting Cyber Incidents	§ 1580.325 § 1582.325 § 1584.107 § 1586.325	$292.4	Owner/operators are required to report cybersecurity incidents to CISA.

NPRM Requirements	49 CFR	Ten-Year Costs	Description
Cybersecurity Incident Response Plan (CIRP)	§ 1580.327 § 1582.227 § 1586.227	$60,882.5	CIRP requirements include having a plan to ensure the impacts of a cybersecurity incident are limited and do not spread throughout the system, back-up data is tested before it is used for recovery, measures are in place to ensure isolation of technology to reduce risks, and identification of who, by position, is responsible for implementing measures in the plan. TSA would continue to require owner/operators to test their plans through exercises and modify the CIRP based on the results of the exercises.
Cybersecurity Assessment Plan (CAP)	§ 1580.329 § 1582.229 § 1586.229	$40,238.4	The CAP includes cybersecurity architecture design review and also requires owner/operators to use other assessment capabilities intended to test the effectiveness of their cybersecurity measures. The CAP must include a specific schedule for the assessments to ensure that at least 30 percent of the COIP is tested each year and at a pace to ensure 100 percent is tested every three years.
Documentation to establish compliance	§ 1580.331 § 1582.231 § 1586.231	$8,531.4	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.
Physical Security Coordinator	§ 1586.103	$31.9	Each owner/operator 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.
Reporting of Significant Physical Security Concerns[25]	§ 1586.105	$659.5	Each owner/operator must report, within 24 hours of initial discovery, any potential threats and significant physical security concerns involving transportation-related operations and other potential threats or significant physical security concerns.

Table ES - 2 below displays the total cost of the proposed rule by entity. TSA estimates the ten-year total cost to be $3.1 billion undiscounted, $2.6 billion discounted at 3 percent, and $2.2 billion discounted at 7 percent. The cost to the regulated industries (all four surface transportation modes) comprises approximately 99 percent of the total costs of the proposed rule, while TSA incurs the remaining portion of the total cost.

[25] Physical security requirements, including designation of a physical security coordinator and reporting of significant physical security concerns are already applicable to Freight Rail, PTPR, and OTRB industries under TSA's Security Training rulemaking. New costs are only associated with the Pipeline industry.

Table ES - 2: Total Cost of the Proposed Rule by Entity ($ Thousands)

Year	Industry				Total Regulated Industries Cost	TSA Cost	Total Cost Under Proposed Rule		
	Pipelines	Freight Rail	PTPR	OTRB			g = ∑e,f		
	a	b	c	d	e = ∑a,b,c,d	f	Undiscounted	Discounted at 3%	Discounted at 7%
1	$85,636.2	$97,652.0	$119,996.3	$188.5	$303,473.1	$4,426.4	$307,899.5	$298,931.5	$287,756.5
2	$81,122.2	$95,471.4	$120,633.3	$6.0	$297,232.9	$2,407.7	$299,640.5	$282,439.9	$261,717.6
3	$79,132.0	$94,622.4	$121,507.8	$6.1	$295,268.4	$2,412.2	$297,680.6	$272,419.9	$242,996.0
4	$82,232.4	$97,002.7	$123,882.8	$6.3	$303,124.3	$1,358.2	$304,482.5	$270,528.8	$232,288.2
5	$80,265.1	$96,187.3	$124,813.9	$6.4	$301,272.8	$1,363.0	$302,635.8	$261,056.3	$215,775.1
6	$83,508.6	$98,675.1	$127,288.7	$6.6	$309,479.0	$1,367.6	$310,846.6	$260,329.1	$207,130.2
7	$81,564.9	$97,885.3	$128,279.4	$6.8	$307,736.3	$1,372.3	$309,108.6	$251,333.6	$192,497.3
8	$84,832.8	$100,405.1	$130,820.6	$6.9	$316,065.4	$1,377.2	$317,442.6	$250,592.2	$184,754.5
9	$82,913.9	$99,647.7	$131,873.8	$7.1	$314,442.5	$1,382.0	$315,824.5	$242,053.2	$171,787.6
10	$86,207.0	$102,200.5	$134,484.0	$7.3	$322,898.8	$1,387.1	$324,285.9	$241,299.2	$164,850.5
Total	**$827,415.1**	**$979,749.6**	**$1,263,580.7**	**$247.9**	**$3,070,993.4**	**$18,853.8**	**$3,089,847.2**	**$2,630,983.7**	**$2,161,553.8**
Annualized								**$308,431.6**	**$307,756.6**

Note: Totals may not add due to rounding.

Table ES - 3 displays the ten-year cost to the freight rail industry to be $979.8 million undiscounted, $834.5 million discounted at 3 percent, and $685.8 million discounted at 7 percent.

Table ES - 3: Total Cost of the Proposed Rule to the Freight Rail Industry ($ Thousands)

Year	Familiarization	CRM Program				Reporting Cybersecurity Incidents	CIRP	Total Cost		
		CSE	COIP	CAP	Recordkeeping and Compliance			h = ∑a,b,c,d,e,f, g		
	a	b	c	d	e	f	g	Undiscounted	Discounted at 3%	Discounted at 7%
1	$242.2	$233.2	$94,080.9	$855.2	$276.4	$1.0	$1,963.1	$97,652.0	$94,807.8	$91,263.6
2	$2.0	$235.0	$91,019.3	$2,513.7	$278.6	$1.0	$1,421.7	$95,471.4	$89,990.9	$83,388.4
3	$2.0	$236.8	$91,787.7	$881.4	$280.8	$1.0	$1,432.7	$94,622.4	$86,592.9	$77,240.1
4	$2.0	$238.7	$92,494.0	$2,540.1	$283.0	$1.0	$1,444.0	$97,002.7	$86,185.7	$74,002.9
5	$2.0	$240.6	$93,294.9	$908.3	$285.2	$1.0	$1,455.4	$96,187.3	$82,972.1	$68,580.3
6	$2.0	$242.4	$94,108.1	$2,567.3	$287.4	$1.0	$1,466.8	$98,675.1	$82,638.8	$65,751.4
7	$2.0	$244.3	$94,934.6	$935.4	$289.7	$1.0	$1,478.1	$97,885.3	$79,589.7	$60,958.0
8	$2.1	$246.3	$95,779.5	$2,594.6	$291.9	$1.1	$1,489.8	$100,405.1	$79,260.7	$58,436.7
9	$2.1	$248.2	$96,637.8	$963.1	$294.2	$1.1	$1,501.3	$99,647.7	$76,371.7	$54,201.8
10	$2.1	$250.1	$97,515.2	$2,622.3	$296.5	$1.1	$1,513.2	$102,200.5	$76,046.8	$51,953.6
Total	**$260.3**	**$2,415.6**	**$941,652.1**	**$17,381.5**	**$2,863.6**	**$10.3**	**$15,166.2**	**$979,749.6**	**$834,457.1**	**$685,776.6**
Annualized									**$97,823.8**	**$97,639.2**

Note: Totals may not add due to rounding.

Table ES - 4 displays the ten-year cost to the PTPR industry to be $1.26 billion undiscounted, $1.07 billion discounted at 3 percent, and $881.1 million discounted at 7 percent.

Table ES - 4: Total Cost of the Proposed Rule to the PTPR Industry ($ Thousands)

Year	Familiarization	CRM Program				Reporting Cyber-security Incidents	CIRP	Total Cost		
		CSE	COIP	CAP	Recordkeeping and Compliance			h = ∑a,b,c,d,e,f,g		
	a	b	c	d	e	f	g	Undiscounted	Discounted at 3%	Discounted at 7%
1	$54.5	$103.3	$118,492.8	$388.8	$84.2	$1.3	$871.4	$119,996.3	$116,501.3	$112,146.1
2	$1.2	$105.5	$118,601.2	$1,163.5	$86.1	$1.3	$674.5	$120,633.3	$113,708.5	$105,365.8
3	$1.2	$107.9	$120,197.1	$422.7	$88.0	$1.3	$689.6	$121,507.8	$111,196.9	$99,186.6
4	$1.2	$110.2	$121,777.2	$1,198.5	$89.9	$1.3	$704.4	$123,882.8	$110,068.3	$94,509.6
5	$1.3	$112.7	$123,428.7	$458.0	$91.9	$1.4	$720.0	$124,813.9	$107,665.6	$88,990.6
6	$1.3	$115.1	$125,106.4	$1,234.9	$93.9	$1.4	$735.7	$127,288.7	$106,602.3	$84,817.9
7	$1.3	$117.6	$126,816.2	$495.0	$95.9	$1.4	$751.8	$128,279.4	$104,302.9	$79,886.0
8	$1.4	$120.2	$128,558.3	$1,272.8	$98.0	$1.5	$768.3	$130,820.6	$103,271.0	$76,138.8
9	$1.4	$122.8	$130,329.1	$533.7	$100.2	$1.5	$785.0	$131,873.8	$101,070.3	$71,730.6
10	$1.4	$125.5	$132,138.6	$1,312.2	$102.4	$1.5	$802.3	$134,484.0	$100,068.7	$68,364.9
Total	**$66.3**	**$1,140.9**	**$1,245,445.7**	**$8,480.3**	**$930.5**	**$14.0**	**$7,503.1**	**$1,263,580.7**	**$1,074,455.7**	**$881,136.8**
Annualized									**$125,959.0**	**$125,454.1**

Note: Totals may not add due to rounding.

OTRB owner/operators incur the least costs among industries since they only have the reporting requirement. Table ES - 5 displays the ten-year cost to the OTRB industry to be $0.25 million undiscounted, $0.23 million discounted at 3 percent, and $0.22 million discounted at 7 percent.

Table ES - 5: Total Cost of the Proposed Rule to the OTRB Industry ($ Thousands)

Year	Familiarization	Reporting Cybersecurity Incidents	Total OTRB Cost		
			c=∑a,b		
	a	b	Undiscounted	Discounted at 3%	Discounted at 7%
1	$187.2	$1.3	$188.5	$183.0	$176.2
2	$4.7	$1.3	$6.0	$5.6	$5.2
3	$4.8	$1.3	$6.1	$5.6	$5.0
4	$4.9	$1.4	$6.3	$5.6	$4.8
5	$5.0	$1.4	$6.4	$5.5	$4.6
6	$5.2	$1.4	$6.6	$5.5	$4.4
7	$5.3	$1.5	$6.8	$5.5	$4.2
8	$5.4	$1.5	$6.9	$5.5	$4.0
9	$5.6	$1.5	$7.1	$5.4	$3.9
10	$5.7	$1.6	$7.3	$5.4	$3.7
Total	**$233.8**	**$14.1**	**$247.9**	**$232.7**	**$215.9**
Annualized				**$27.3**	**$30.7**

Note: Totals may not add due to rounding.

Pipeline owner/operator costs are shown below in Table ES - 6. This table displays the ten-year cost to the pipeline to be $827.4 million undiscounted, $705.2 million discounted at 3 percent, and $580.2 million discounted at 7 percent.

Table ES - 6: Total Cost of the Proposed Rule to the Pipeline Industry ($ Thousands)

Year	Familiariz-ation	Physical Security Costs	CRM Program				Reporting Cyber-security Incidents	CIRP	Total Cost		
			CSE	COIP	CAP	Recordkeeping and Compliance			i = ∑a,b,c,d,e,f,g,h		
	a	b	c	d	e	f	g	h	Undiscounted	Discounted at 3%	Discounted at 7%
1	$911.6	$37.0	$973.1	$74,786.3	$1,359.2	$644.6	$37.8	$6,886.5	$85,636.2	$83,141.9	$80,033.8
2	$0.0	$21.4	$973.1	$69,414.8	$3,958.8	$644.6	$37.8	$6,071.7	$81,122.2	$76,465.5	$70,855.3
3	$0.0	$21.4	$973.1	$70,024.2	$1,359.2	$644.6	$37.8	$6,071.7	$79,132.0	$72,417.0	$64,595.3
4	$0.0	$21.4	$973.1	$70,525.0	$3,958.8	$644.6	$37.8	$6,071.7	$82,232.4	$73,062.4	$62,734.7
5	$0.0	$21.4	$973.1	$71,157.2	$1,359.2	$644.6	$37.8	$6,071.7	$80,265.1	$69,237.4	$57,227.9
6	$0.0	$21.4	$973.1	$71,801.1	$3,958.8	$644.6	$37.8	$6,071.7	$83,508.6	$69,937.1	$55,645.3
7	$0.0	$21.4	$973.1	$72,457.0	$1,359.2	$644.6	$37.8	$6,071.7	$81,564.9	$66,319.7	$50,794.5
8	$0.0	$21.4	$973.1	$73,125.3	$3,958.8	$644.6	$37.8	$6,071.7	$84,832.8	$66,967.8	$49,373.5
9	$0.0	$21.4	$973.1	$73,806.0	$1,359.2	$644.6	$37.8	$6,071.7	$82,913.9	$63,546.6	$45,099.7
10	$0.0	$21.4	$973.1	$74,499.5	$3,958.8	$644.6	$37.8	$6,071.7	$86,207.0	$64,146.1	$43,823.3
Total	**$911.6**	**$229.6**	**$9,731.4**	**$721,596.4**	**$26,590.3**	**$6,446.0**	**$378.4**	**$61,531.4**	**$827,415.1**	**$705,241.5**	**$580,183.2**
Annualized										**$82,675.8**	**$82,605.0**

Note: Totals may not add due to rounding.

The TSA burden would be for reviewing the CRM programs and keeping track of key personnel. TSA will incur ongoing costs with the implementation of this rulemaking. Table ES - 7 displays the ten-year cost to TSA to be $18.9 million undiscounted, $16.6 million discounted at 3 percent, and $14.2 million discounted at 7 percent.

Table ES - 7 : Total Cost of the Proposed Rule to TSA ($ Thousands)

Year	Physical Security Costs	CRM Program			CIRP	Total Costs		
		CSE	COIP	CAP		f = ∑a,b,c,d,e		
	a	b	c	d	e	Undiscounted	Discounted at 3%	Discounted at 7%
1	$75.0	$71.5	$3,435.6	$572.2	$272.3	$4,426.4	$4,297.5	$4,136.9
2	$75.0	$71.9	$1,484.0	$575.5	$201.3	$2,407.7	$2,269.5	$2,102.9
3	$75.0	$72.4	$1,484.5	$579.0	$201.4	$2,412.2	$2,207.5	$1,969.1
4	$75.0	$72.8	$426.5	$582.5	$201.5	$1,358.2	$1,206.8	$1,036.2
5	$75.0	$73.3	$427.1	$586.0	$201.6	$1,363.0	$1,175.7	$971.8
6	$75.0	$73.7	$427.6	$589.7	$201.7	$1,367.6	$1,145.3	$911.3
7	$75.0	$74.2	$428.0	$593.3	$201.8	$1,372.3	$1,115.8	$854.6
8	$75.0	$74.6	$428.6	$597.1	$202.0	$1,377.2	$1,087.2	$801.6
9	$75.0	$75.1	$429.0	$600.8	$202.1	$1,382.0	$1,059.2	$751.7
10	$75.0	$75.6	$429.7	$604.7	$202.2	$1,387.1	$1,032.1	$705.1
Total	**$749.6**	**$735.1**	**$9,400.6**	**$5,880.7**	**$2,087.9**	**$18,853.8**	**$16,596.7**	**$14,241.2**
Annualized							**$1,945.6**	**$2,027.6**

Note: Totals may not add due to rounding.

Benefits of the Proposed Rule

The proposed rule would enhance cybersecurity by reducing vulnerability to cyber-incidents and strengthening response measures in the event of a cybersecurity incident. Having strong defense mechanisms in place supports and increases company confidence in their abilities to monitor threats and mitigate any damages. Specifically, the proposed rule would require designated owner/operators for all four modes to report cybersecurity incidents. Designated owner/operators of freight railroads, PTPR, and pipeline facilities and systems would also be required to identify a cybersecurity coordinator as well as develop and implement a comprehensive CRM program. The proposed CRM program includes three primary elements. First, owner/operators would be required to regularly conduct an enterprise-wide cybersecurity evaluation that would identify the current profile of cybersecurity. This serves as a starting point to build out a larger CRM program and provides an understanding of one's cybersecurity profile over time. Second, owner/operators would be required to develop a COIP with requirements that focus on: (a) governance of the CRM program, (b) identification of Critical Cyber Systems; (c) protecting Critical Cyber Systems; (d) detecting and monitoring Critical Cyber Systems; and (e) ensuring response and recovery. This helps outline an owner/operator's strategy to address cybersecurity and describes how mitigation measures and activities will function. As part of the COIP process to ensure response and recovery, owner/operators would develop a CIRP that requires an established set of policies and procedures in place to respond to intrusions into their critical cybersecurity systems as well as maintenance or reconstitution of operations during an incident. Having such plans in place reduce time and confusion when responding to incidents which provides 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. This helps provide an overview of vulnerabilities, the nature of potential exploits, and a roadmap for how to fix such vulnerabilities which helps improve effectiveness and maintain accountability. The rule would also expand the requirement for having a physical security coordinator (currently in 49 CFR 1570.201) and reporting physical security incidents (currently in 49 CFR 1570.203) to owner/operators of designated pipeline facilities and systems.

Implementation of these requirements would likely result in qualitative benefits to affected owner/operators. For instance, by having a standardized requirement applicable to all owner/operators that meet applicability criteria, there would be more consistent application of requirements and increased investments in cybersecurity measures. Further, as the plans are implemented, there are expected gains in efficiencies over time as covered owner/operators refine and improve their systems. The primary benefit of the CRM program is a reduction in the risk of successful cybersecurity incidents as well as the impact of such an incident. Requirements of the proposed rule would help enhance security of the regulated population which reduces negative consequences and service interruptions for surface modes like freight railroad, passenger railroad, and pipelines thereby benefiting owners/operators, passengers, and consumers. Such benefits are difficult to quantify given the wide range of applicable entities with varying levels of complexity and specialized operational technology (OT) equipment, ever-changing IT systems and uncertainty surrounding how frequent cybersecurity threats or incidents may occur and through what mechanisms. Therefore, TSA includes a break-even analysis to compare the potential security benefits of the CRM Program with its estimated cost to implement.

Break-Even Analysis

In addition to a qualitative discussion of benefits, 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 implementing the rule. 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?"

To conduct the break-even analysis, TSA evaluates a selection of potential consequence levels for each of the modes covered by the proposed rule, excluding OTRB who is not required to implement CRM requirements (only reporting cybersecurity incidents). TSA also provides illustrative examples of the type of incident that could result in a similar level of damage or consequence for each mode of transportation and the examples provided represent the type of security incidents that may occur but neither include all possible attacks or incidents nor suggest that the identified situations are the most likely or represent the highest vulnerability to a cybersecurity incident. TSA uses this approach due to the uncertain yet growing threat associated with cyber incidents.[26]

Cyber-attacks are typically focused on denial of service or business disruption, data breach of internal information, and infrastructure/asset manipulation which in some cases have monetary implications. Each type of attack may result in different direct and indirect consequences including damage, loss of life, incident response, delay of services, and added inefficiencies

[26] Additional discussion on potential cybersecurity threats can be found in Section 1.3 Need for Regulatory Action.

(e.g., having to ship products via alternative more expensive means).[27] Such attack's impacts can be amplified or reduced based on specific circumstances of the event. For example, smaller versus larger/multiple targets, duration of disruption, as well as severity of outcomes (e.g., derailing trains in an open non-populated area versus a bridge, tunnel, or city center) impact the level of consequence. As such, there are a wide range of events that a CRM program can help protect against, from small incidents like targeted ransomware attacks and data breaches to large incidents like complex network attacks that take operations offline for extended periods of time.

The simplest version of the conclusion is that if the proposed rule prevents annual costs of approximately $307.8 million (at 7%) across all impacted surface modes, its benefits will justify its costs. However, TSA also performed a sensitivity analysis of key industry costs drivers to help account for uncertainty and potential current industry practices. Based on these reduced costs, the proposed rule would only need to prevent annual costs of approximately $185.0 million. TSA's break-even analysis evaluates the cybersecurity provisions of the rule across modes which require the prevention of annual costs of approximately $98.2 million ($65.6 million under sensitivity estimates) for freight rail, $125.7 million ($76.6 million under sensitivity estimates) for PTPR, and $83.7 million ($63.2 million under sensitivity estimates) for pipelines (discounted at 7 percent) to break even. Taking into account 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.

---

[27] Direct consequences capture economic losses that can be clearly linked to an incident without intermediate connections (e.g., the replacement cost of a train for an incident that causes a train derailment). Indirect consequences capture economic losses that are caused or augmented by an incident but a couple steps removed (e.g., the need to re-route trains due to an incident that causes a train derailment).

A break-even analysis estimates a threshold value for the security benefits of the proposed rule so that the benefits of the rule 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. A more detailed review of potential consequence levels considered in the break-even analysis with some illustrative examples can be found in Section 4.2 of the TSA CRM Preliminary Regulatory Impact Analysis (RIA). However, Table ES - 8 presents a summary of break-even levels for the full cost of the CRM program across potential consequence levels for each of the covered modes of transportation. It, however, does not include an evaluation of OTRB costs whose requirement is only for incident reporting nor pipeline physical security requirements.

Table ES - 8: 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 Incident
		a	b	c = a ÷ b	d = b ÷ a
Freight Rail	$1 Billion Example	$98.22 million	$1 billion	0.0982	One every 10.18 years
	$10 Billion Example		$10 billion	0.0098	One every 101.81 years
	$20 Billion Example		$20 billion	0.0049	One every 203.62 years
PTPR	$1 Billion Example	$125.74 million	$1 billion	0.1257	One every 7.95 years
	$2.5 Billion Example		$2.5 billion	0.0503	One every 19.88 years
	$5 Billion Example		$5 billion	0.0251	One every 39.76 years
Pipeline	$2 Billion Example	$83.691 million	$2 billion	0.0418	One every 23.9 years
	$10 Billion Example		$10 billion	0.0084	One every 119.49 years
	$20 Billion Example		$20 billion	0.0042	One every 238.98 years

TSA also performed a sensitivity analysis of key industry costs drivers which helps accounts for uncertainty and potential current industry practices. Table ES - 9 presents a summary of break-even levels using the reduced cost estimates from TSA's sensitivity analysis across potential consequence levels for each of the covered modes of transportation.

Table ES - 9: 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 Incident
		a	b	c = a ÷ b	d = b ÷ a
Freight Rail	$1 Billion Example	$65.575 million	$1 billion	0.0656	One every 15.25 years
	$10 Billion Example		$10 billion	0.0066	One every 152.5 years
	$20 Billion Example		$20 billion	0.0033	One every 304.99 years
PTPR	$1 Billion Example	$76.552 million	$1 billion	0.0766	One every 13.06 years
	$2.5 Billion Example		$2.5 billion	0.0306	One every 32.66 years
	$5 Billion Example		$5 billion	0.0153	One every 65.31 years
Pipeline	$2 Billion Example	$63.222 million	$2 billion	0.0316	One every 31.63 years
	$10 Billion Example		$10 billion	0.0063	One every 158.17 years
	$20 Billion Example		$20 billion	0.0032	One every 316.35 years

Accounting Statement

The OMB A-4 Accounting Statement in Table ES - 10 presents annualized costs and qualitative benefits of the proposed rule in 2022 dollars.

Table ES - 10: OMB A-4 Accounting Statement ($ Millions, 2022 Dollars)

Category	Estimates			Units			Notes
	Primary Estimate	Low Estimate	High Estimate	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, would 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	Not Quantified
	N/A	N/A	N/A	N/A	3%	N/A	

Category	Estimates			Units			Notes
	Primary Estimate	Low Estimate	High Estimate	Year Dollar	Discount Rate	Period Covered	
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 implementation process beyond what TSA has estimated.						
Transfers							
Annualized Monetized transfers: Employer compensation transfers ($ millions/year)	N/A	N/A	N/A	N/A	7%	N/A	N/A
	N/A	N/A	N/A	N/A	3%	N/A	
From/To	From:	Displaced Employees		To:	Replacement Labor		
Annualized Monetized transfers: Unemployment transfer payment to employees ($ millions/year)	N/A	N/A	N/A	N/A	7%	N/A	N/A
	N/A	N/A	N/A	N/A	3%	N/A	
From/To	From:	States		To:	Displaced Employees		
Annualized Monetized transfers: A reduction in employment taxes transfer payments ($ millions/year)	N/A	N/A	N/A	N/A	7%	N/A	N/A
	N/A	N/A	N/A	N/A	3%	N/A	
From/To	From:	Employers and Displaced Employees		To:	Federal Government		
Other Annualized Monetized ($ millions/year)	N/A	N/A	N/A	N/A	7%	N/A	N/A
	N/A	N/A	N/A	N/A	3%	N/A	
From/To	From:	N/A		To:	N/A		
Effects On							
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.						N/A
Small Business	Prepared IRFA.						NPRM IRFA
Wages	None.						N/A
Growth	Not Measured.						

Alternatives Considered

In addition to the proposed rule, or the "preferred alternative," TSA also considered three alternative regulatory options. The first alternative (Alternative 1) is to implement a limited

scope of requirements. Alternative 1 would limit the rule to the requirements associated with Governance of the CRM, Cybersecurity Coordinator, Identification of Critical Cybersecurity Systems, Reporting Cybersecurity Incidents, and the CIRP.

These requirements identify responsible persons and organizations for an owner/operators CRM program, identify the cybersecurity systems, require the reporting of cybersecurity incidents to CISA, and require the submission of a CIRP. Any other security requirements or program implementation would be up to the owner/operator to establish and implement voluntarily for themselves. This alternative is largely based on existing SD criteria and would enable TSA to maintain oversight at a reactionary level, but, although being less costly, it would reduce visibility of any preventative efforts owner/operators are undertaking.

The second alternative (Alternative 2) is to reduce the applicability of the rule across the industries being regulated. Alternative 2 would adjust the applicability of the requirements to cover a smaller portion of 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 only six owner/operators being impacted versus 73 in the preferred alternative. 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 three years or at any time in the future. This covers 27 owner/operators, down from 34 in the preferred alternative. For the regulated pipeline owner/operators, it would cover the 98 most critical owner/operators of hazardous liquid and natural gas pipelines and liquefied natural gas facilities.

The third alternative (Alternative 3) is to add a vetting requirement for cybersecurity

coordinators and accountable executives in all covered modes as well as frontline workers for pipeline entities. Alternative 3 would introduce a requirement for accountable executives and cybersecurity coordinators, in all covered entities, to receive a Level 3 Security Threat Assessment (STA). 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.[28]

Table ES - 11 presents a comparison of the costs between the proposed rule (preferred alternative) and the alternatives considered.

[28] *See* Vetting of Certain Surface Transportation Employees Notice of Proposed Rulemaking. Docket ID: TSA-2023-0001 at https://www.regulations.gov/docket/TSA-2023-0001. Accessed on July 5, 2023.

Table ES - 11: Comparison of Costs Between the Proposed Rule and Alternatives (Discounted at 7%, $ Thousands)

Regulatory Action	Initial Affected Population (Number of Entities)	Requirements	10-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	All requirements in the Proposed Rule	$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	Governance of the CRM, Cybersecurity Coordinator, Identification of Critical Cybersecurity Systems, Reporting Cybersecurity Incidents, and the Cybersecurity Incident Response Plan	$76,963	$2,391	$79,354	$10,958	$340	$11,298
Alternative 2	Freight Rail – 6 PTPR – 27 OTRB – 71 Pipeline - 98	All requirements in the Proposed Rule	$1,589,258	$11,085	$1,600,343	$226,275	$1,578	$227,853
Alternative 3	Freight Rail – 73 PTPR – 34 OTRB – 71 Pipeline - 115	All requirements in the Proposed Rule plus for accountable executives and cybersecurity coordinators, in all covered entities, to receive a Level 3 Security Threat Assessment (STA). Furthermore, this alternative would require all frontline workers ("security-sensitive employees") in the pipeline industry to undergo a Level-2 STA	$2,160,147	$14,241	$2,174,388	$307,556	$2,028	$309,584

Note: Totals may not add due to rounding.

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 in addressing cybersecurity. Based on insight from 2021/2022 owner/operator self-assessments from initial cybersecurity SDs as well as previous industry engagement, the industry did not appear to be sufficiently implementing preventative measures on its own. Limiting the scope of the requirements, as Alternative 1 does, would not produce the desired outcome regarding reduced cybersecurity risk as discussed in the need for the rule section (Section 1.3) and associated benefits section (Section 4.1). Alternative 2 also has a smaller cost. However, it too does not achieve desired risk reductions as it fails to cover many entities TSA considers important due to their interaction with the nation-wide systems and whose operational disruption may have cascading effects. TSA finds this risk to be an issue of national security based on the role these industries play in the supply chain, movement of people and goods, and the economy as a whole. Regulating only the large members of the supply chain and ensuring their cybersecurity is effective has a reduced impact if the smaller companies they engage with are unable to function due to cybersecurity incidents the proposed regulation is designed to counter. Alternative 3 is costlier than the proposed rule due to the additional vetting requirements for cybersecurity coordinators and accountable executives across modes as well as pipeline frontline employees. 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 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.

Initial Regulatory Flexibility Analysis

TSA has performed an Initial Regulatory Flexibility Analysis (IRFA) of the impacts on small entities, including small businesses, from this proposed rule. TSA found the proposed rule may affect an estimated 293 entities (73 corporate-level freight railroads; 34 PTPR agencies; 71 OTRB owner/operators; and 115 pipeline owner/operators).[29] These entities include businesses and governmental jurisdictions. TSA did not find any non-profit organizations affected by this proposed rule. TSA estimates that 79 (27 percent) are considered small entities. More specifically, TSA estimates that 17 freight railroads (23 percent), 0 PTPR agencies (0 percent), 55 OTRB owner/operators (78 percent), and 7 pipeline owner/operators (6 percent) are considered small entities.

Regulated entities have different requirements under the proposed rule, depending on their industry. Freight railroad, PTPR, and Pipeline owner/operators would be required to designate a cybersecurity coordinator, report cybersecurity incidents, and have a Cybersecurity Risk Management (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 physical security incidents to TSA. OTRB owner/operators only have to report cybersecurity incidents to CISA, as well as incur familiarization costs.

[29] See Section 2.1 for a detailed discussion on the initial number of regulated freight rail entities, PTPR agencies, OTRB owner/operators, and pipeline owner/operators.

TSA estimates an average proposed rule per entity cost of $486,792 per freight rail entity, $682 per OTRB entity, and $484,848 per pipeline entity across each of the proposed rule provisions. Cost breakout detail can be found in Chapter 6, specifically in Tables 6-2 for Freight, 6-6 for OTRB, and 6-9 for Pipeline. In addition, TSA estimates a $537 per employee for freight rail entities and $659 per employee for pipeline entities.[30] Both are from the highest cost year of the proposed rule (year 10 undiscounted). 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 railroads, 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 of them. As shown in the IRFA, 11 of the analyzed entities would have an impact greater than 1 percent of their annual revenue, with 4 of them having impacts on revenue of 5 or more percent. Of these impacted small entities, all are freight rail owner/operators. None of the PTPR entities are considered small, and the requirements in the proposed rule for OTRB entities, being more limited than the requirements for the other modes, do not have an impact greater than 1% of revenue on any covered entities in that mode. Seven pipeline owner/operators are considered small, but none have cost impacts greater than 1% of annual revenue in the highest cost year.

[30] The per employee costs provided in this analysis are for Freight Railroad and Pipeline owner/operators only, since none of the PTPR owner/operators are small and there are no per employee costs for OTRB owner/operators in the proposed rule.

Table ES - 12: Number and Percentage of Affected Small Entities by Mode

Revenue Impact Range	Freight Rail Number of Affected Small Entities	Freight Rail Percentage of Affected Small Entities	OTRB Number of Affected Small Entities	OTRB Percentage of Affected Small Entities	Pipeline Number of Affected Small Entities	Pipeline Percentage of Affected Small Entities	Total Number of Affected Small Entities	Total Percentage 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%**

Paperwork Reduction Act

The Paperwork Reduction Act of 1995 (PRA) (44 U.S.C. 3501. et seq.) requires that TSA consider the impact of paperwork and other information collection burdens imposed on the public and, under the provisions of 44 U.S.C. § 3507(d), obtain approval from OMB for each collection of information it conducts, sponsors, or requires through regulations. Table ES - 13 shows the information collection and corresponding burden-hours for entities falling under the requirements of the proposed rule. There are many collections that have been implemented under the SD related ICRs and would continue or be updated under the proposed rule.[31] The time burdens associated with new collections of information are reflected in the Table ES - 13.

Table ES - 13: PRA Burden of Hours

Information Collection Activity by Mode	Number of Responses			Time Per Response (hours)	Time Burden			3-Year Time Burden	Average Annual Time Burden/Responses
	Year 1	Year 2	Year 3		Year 1	Year 2	Year 3		
	a	b	c	d	e = a × d	f = b × d	g = c × d	h = e + f + g	i = h ÷ 3
Cybersecurity Evaluation (CSE)									
Freight Rail	73.00	73.6	74.1	40.00	2,920	2,943	2,966	8,828	2,943
PTPR	34.00	34.7	35.5	40.00	1,360	1,390	1,420	4,170	1,390

[31] OMB previously approved information collection requests 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.

Information Collection Activity by Mode	Number of Responses			Time Per Response (hours)	Time Burden			3-Year Time Burden	Average Annual Time Burden/Responses
	Year 1	Year 2	Year 3		Year 1	Year 2	Year 3		
	a	b	c	d	e = a × d	f = b × d	g = c × d	h = e + f + g	i = h ÷ 3
Pipelines	115.00	115.00	115.00	120.00	13,800	3,800	13,800	41,400	13,800
Submit COIP									
Freight Rail	73.00	-	0.6	40.00	2,920	-	24	2,944	981
PTPR	34.00	-	0.7	40.00	1,360	-	28	1,388	463
Pipelines	115.00	-	-	40.00	4,600	-	-	4,600	1,533
Update COIP									
Freight Rail	-	73	73.6	13.30	-	971	978	1,949	650
PTPR	-	34	34.7	13.30	-	452	462	914	305
Pipelines	-	115	115	13.30	-	1,530	1,530	3,059	1,020
Initial Identification of Critical Cyber Systems									
Freight Rail	73.00	0.57	0.57	160.00	11,680	91	91	11,862	3,954.13
PTPR	34.00	0.74	0.77	160.00	5,440	118	123	5,682	1,893.87
Pipelines	115.00	-	-	160.00	18,400	-	-	18,400	6,133.33
Annual Identification of Critical Cyber Systems									
Freight Rail	73.00	73.00	73.57	40.00	2,920	2,920	2,943	8,783	2,927.60
PTPR	34.00	34.74	35.51	40.00	1,360	1,390	1,420	4,170	1,390.00
Pipelines	115.00	115.00	115.00	40.00	4,600	4,600	4,600	13,800	4,600.00
Submit POAM									
Freight Rail	14.60	14.71	14.83	80.00	1,168	1,177	1,186	3,531	1,177
PTPR	6.80	6.95	7.10	80.00	544	556	568	1,668	556
Pipelines	23.00	23.00	23.00	80.00	1,840	1,840	1,840	5,520	1,840
Accountable Executive Information Submission									
Freight Rail	73.00	3.51	3.55	3.00	219	11	11	240	80
PTPR	34.00	5.24	5.37	3.00	102	16	16	134	45
Pipelines	115.00	15.72	15.72	3.00	345	47	47	439	146
Cybersecurity Coordinator Information Submission									
Freight Rail	146.00	7.03	7.07	2.00	292	14	14	320	107
PTPR	68.00	10.48	10.74	2.00	136	21	21	178	59
Pipelines	230.00	31.44	31.44	2.00	460	63	63	586	195
Supply Chain Management									
Freight Rail	73.00	73.57	74.14	10.00	730	736	741	2,207	736
PTPR	34.00	34.74	35.51	10.00	340	347	355	1,043	348
Pipelines	115.00	115.00	115.00	10.00	1,150	1,150	1,150	3,450	1,150
Physical Security Coordinator Information Submission									
Pipelines	261.05	35.69	35.69	0.50	131	18	18	166	55
Report Physical Security Incidents to TSA									
Pipelines	2,908.35	2,908.35	2,908.35	0.05	145	145	145	436	145
Initial Cybersecurity Training Plan Development and Submission									
Freight Rail	73.00	0.57	0.57	80.00	5,840	46	46	5,931	1,977
PTPR	34.00	0.74	0.77	80.00	2,720	59	62	2,841	947
Pipelines	115.00	-	-	80.00	9,200	-	-	9,200	3,067
Cybersecurity Training Documentation Recordkeeping									
Freight Rail	134,504.00	135,068.91	135,636.21	0.02	2,690	2,701	2,713	8,104	2,701
PTPR	344,632.00	348,457.42	352,325.29	0.02	6,893	6,969	7,047	20,908	6,969
Pipelines	45,908.00	46,192.63	46,479.02	0.02	918	924	930	2,772	924
Report Cybersecurity Incidents to CISA									
Freight Rail	10.22	10.31	10.39	1.00	10	10	10	31	10
PTPR	14.96	15.29	15.62	1.00	15	15	16	46	15
OTRB	14.91	15.28	15.66	1.00	15	15	16	46	15

Information Collection Activity by Mode	Number of Responses			Time Per Response (hours)	Time Burden			3-Year Time Burden	Average Annual Time Burden/Responses
	Year 1	Year 2	Year 3		Year 1	Year 2	Year 3		
	a	b	c	d	e = a × d	f = b × d	g = c × d	h = e + f + g	i = h ÷ 3
Pipelines	400.20	400.20	400.20	1.00	400	400	400	1,201	400
Cybersecurity Incident Response Plan (CIRP)									
Freight Rail	73.00			80.00	5,840	-	-	5,840	1,947
PTPR	34.00			80.00	2,720	-	-	2,720	907
Pipelines	115.00			80.00	9,200	-	-	9,200	3,067
CIRP Testing									
Freight Rail	73.00	73.57	74.14	120.00	8,760	8,828	8,897	26,485	8,828
PTPR	34.00	34.74	35.51	120.00	4,080	4,169	4,261	12,510	4,170
Pipelines	115.00	115.00	115.00	120.00	13,800	13,800	13,800	41,400	13,800
Cybersecurity Assessment Plan (CAP)									
Freight Rail	73.00	73.57	74.14	44.00	3,212	3,237	3,262	9,711	3,237
PTPR	34.00	34.74	35.51	44.00	1,496	1,529	1,562	4,587	1,529
Pipelines	115.00	115.00	115.00	44.00	5,060	5,060	5,060	15,180	5,060
CAP Annual Report of COIP Testing									
Freight Rail	73.00	73.57	74.14	30.00	2,190	2,207	2,224	6,621	2,207
PTPR	34.00	34.74	35.51	30.00	1,020	1,042	1,065	3,128	1,043
Pipelines	115.00	115.00	115.00	30.00	3,450	3,450	3,450	10,350	3,450
Recordkeeping									
Freight Rail	73.00	73.57	74.14	2.00	146	147	148	441	147
PTPR	34.00	34.74	35.51	2.00	68	69	71	209	70
Pipelines	115.00	115.00	115.00	2.00	230	230	230	690	230
Total Responses	**531,806**	**535,009**	**539,745**					**1,606,115**	**535,372**
Total Time Burden (Hours)					**168,935**	**91,254**	**91,831**	**352,020**	**117,340**

Note: Totals may not add due to rounding.

1 INTRODUCTION

This Preliminary Regulatory Impact Analysis (RIA) provides supporting documentation and analysis for the Notice of Proposed Rulemaking (NPRM) of the Transportation Security Administration (TSA) Enhancing Surface Cyber Risk Management (TSA-1652-AA74) rulemaking, also referred to as "the proposed rule" throughout this document. The RIA does not attempt to replicate the regulatory language of the proposed rule or any other supporting documentation; if finalized, the regulatory text, not the text of this or any subsequent RIA, would be legally binding.

Section 1 provides a background around the proposed rule, the need for it, and a description of its content. Section 2 introduces the assumptions and data TSA used to complete this RIA. Section 3 presents a cost analysis of the proposed rule to affected industries and TSA. Section 4 presents a benefit analysis of the proposed rule to affected industries and the traveling public. Section 5 analyzes other policy alternatives considered by TSA and compares them to the proposed rule. Section 6 presents the findings from the Initial Regulatory Flexibility Analysis (IRFA) of the proposed rule. Section 7 details the findings of the additional burden imposed on the public from additional paperwork and record keeping as required by the Paperwork Reduction Act (PRA). Section 8 describes the findings from the International Trade Impact Assessment. Section 9 presents findings from the Unfunded Mandates Reform Act (UMRA) analysis.

1.1 Background

The purpose of this rule is to promote the security of surface transportation systems and associated infrastructure by strengthening cybersecurity across the certain modes within the

Surface Transportation Sector in response to the ongoing cyber threats. The industries affected by this rule are of vital importance to the domestic and global economies. The affected industries (freight rail, passenger rail, rail transit, and pipeline transportation) are responsible for over $265 billion dollars of annual economic output.[32] These modal output levels do not include related industries such as supporting activities for transportation or oil and gas extraction. Freight rail and pipelines are responsible for more than 45 percent of U.S. freight movement by ton-miles.[33] The interconnectivity of these industries to the global economy underscores how valuable and crucial the industries affected by this rule are to a strong economy.

The history of cybersecurity starts in the 1970s when words such as ransomware, spyware, viruses, worms, and logic bombs did not exist; however, advances in technology and increases in cyber threats has placed these terms frequently in today's news headlines.[34] For every benefit of technological innovation and efficiency, such as the ability to perform tasks remotely, there is an added cybersecurity risk as more access points can increase vulnerabilities. In 2018, a study on applications for supervisory control and data acquisition (SCADA), which are used to facilitate remote monitoring of services, found numerous vulnerabilities across the sample, an increase from a 2015 analysis. Cybercriminals could exploit these vulnerabilities to disrupt and/or damage critical infrastructure.[35]

---

[32] Compiled using U.S. Bureau of Economic Analysis data for 2022Q4, including Gross Output by Industry and Table 6.16D. Corporate Profits by industry. See https://apps.bea.gov/iTable/?reqid=19&step=3&isuri=1&1921=survey&1903=239 for Table 6.16D.

[33] U.S. Department of Transportation, 2019 Pocket Guide to Transportation, www.bts.dot.gov/browse-statistical-products-and-data/pocket-guide-transportation/pocket-guide-2019.pdf.

[34] Mutune, George. "The Quick and Dirty History of Cybersecurity" *Cyberexperts*, https://cyberexperts.com/history-of-cybersecurity/. Accessed July 5, 2023

[35] SCADA security: Bad app design could give hackers access to industrial control systems," By Danny Palmer, January 11, 2018. https://www.zdnet.com/article/scada-security-bad-app-design-could-give-hackers-access-to-industrial-control-systems/

Cybersecurity incidents are often highly damaging. In May 2021, a major pipeline operator experienced a ransomware cyber-attack resulting in their decision to shut down their pipeline. The shutdown affected consumers and transportation systems along the U.S. East Coast and increased costs associated with the transportation of millions of barrels of oil by trucks, rails, ships, etc. Actions taken to the 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.[36] The cyber-attack in May 2021 is one of many recent ransomware attacks demonstrating the necessity of ensuring that critical infrastructure is protected and that owner/operators are proactively deploying cybersecurity risk management (CRM) measures. In addition, cyber attackers have maliciously 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.[37] Cyber 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.[38] 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.

---

[36] *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), https://www.fmcsa.dot.gov/emergency/esc-ssc-wsc-regional-emergency-declaration-2021-002-05-09-2021 (last accessed Aug. 1, 2024).

[37] 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.

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

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."[39] 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.[40] 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."[41] 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."[42] Furthermore, "malicious cyber actors have begun testing the capabilities of AI-developed malware 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."[43] Consistent with this information, TSA has also issued SDs to higher-risk freight and passenger rail operations imposing the same requirements issued to pipelines.[44]

---

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

[40] https://www.odni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf (Page 11)

[41] 2023 Intelligence Community Assessment at 10.

[42] 2024 Intelligence Community Assessment at 11.

[43] DHS Intelligence and Analysis (I&A), Homeland Threat Assessment (2024) at 18 (last accessed July 23, 2024, 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).

[44] *See* the SD 1580-2021-01 (first issued December 2021), SD 1582-2021-01 (first issued December 2021, and SD 1580/82-2022-01 series (first issued October 2022).

TSA issued security directives (SDs)[45] 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."[46] These directives include provisions that are carried over to this proposed rulemaking, including having a primary and alternate cybersecurity coordinator, reporting incidents to CISA, and developing a CIRP, among others, while also requiring covered owner/operators to continually assess their cybersecurity posture.

Cybersecurity is a major area of concern across organizations especially given that cybercrime is projected to cost the world trillions of dollars in the coming years, with an estimate from the World Economic Forum indicating the global cost of cybercrime will be almost 14 trillion dollars.[47][48] Mitigating threats facing domestic critical infrastructure, including enhancing the pipeline and rail industry's current cybersecurity risk management posture, has important implications for national and economic security. Cyber actors have demonstrated their

---

[45] See https://www.tsa.gov/for-industry/surface-transportation-cybersecurity-toolkit for links to the SDs. TSA issued these SDs under the specific authority of 49 U.S.C. 114(l)(2)(A). 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 regulation or SD must be issued immediately in order to protect transportation security, the Administrator shall issue the regulation or SD 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.

[46] *See* National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems, available at https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/ (July 28, 2021).

See Cybercrime To Cost The World $10.5 Trillion Annually by 2025, available at https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ (November 13, 2020). Accessed July 15, 2024. Also referenced in USAID Cybersecurity Briefer: Economic Growth and Trade, available at https://www.usaid.gov/digital-development/cybersecurity/economic-growth-briefer (October 17, 2023).

[48] Elliott, David. "FBI takes down army of 'zombie' computers. Here what to know" World Economic Forum. https://www.weforum.org/agenda/2024/06/botnet-cybercrime-zombie-computers/. Accessed July 16, 2024.

willingness to conduct cyber-attacks[49] against critical infrastructure by exploiting the vulnerability of Operational Technology (OT) and Information Technology (IT) systems. For instance, cyber actors attacked the Sacramento Regional Transit system's computers, which affected internal operations, including the ability to use computers to dispatch employees and assign buses for routes.[50] Pipeline and rail systems, and associated facilities, are especially vulnerable to cyber-incidents due to legacy industrial control systems (ICS) that may lack updated security controls and the dispersed nature of pipeline and rail networks spanning urban and outlying areas. Recent U.S. government warnings about Russian, Chinese, and Iranian state-sponsored cyber espionage campaigns to develop capabilities to disrupt U.S. critical infrastructure including the transportation sector highlight the need for action.[51]

As stated previously, transportation companies are vital to the global economy and our health and well-being as a nation. A dependable supply of goods, such as fuel in pipelines and cargo on freight rail, allows an economy to function efficiently. If the public's confidence in availability and reliability is shaken, there can be ripple effects felt throughout the affected industries, and beyond. For instance, if individuals riding public transit become concerned about the safety or dependability of that transit method and cease to utilize it, the resulting impact would be felt across all economic sectors: the opportunity cost of increased commute times, traffic loads on

---

[49] For purposes of this analysis, TSA uses the National Institute of Standards and Technology (NIST) definition of a cyber-attack: An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information. See *https://csrc.nist.gov/glossary/term/cyber_attack*.

[50] Buck, Jon. (2017, November 21). "Hackers attack Sacramento transit system for 1 BTC Ransom," COINTELEGRAPH. https://www.cointelegraph.com/news/hackers-attack-sacramento-transit-system-for-1-btc-ransom

[51] *See, e.g.,* the Annual Threat Assessment of the U.S. Intelligence Community, available at https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf. Accessed on Aug. 1, 2023.

roads and bridges, and the incurred cost of fuel and vehicle wear and tear. There could be more significant effects as well if some individuals opt to leave a job due to lack of safe and reliable transportation. Similarly, fear about availability and accessibility of fuel can have downstream effects. Such fear could lead to individuals hoarding gas which could result in supply runs and further impact fuel availability. Reduced availability could have a number of direct impacts, as well as further cascading impacts especially on the ability to move products via trucking, which is responsible for $12.017 trillion of the $18.907 trillion value of shipments in 2017, or approximately 64 percent of the total.[52] Therefore, a cybersecurity incident that results in destabilization of the transportation industry may result in large and widespread impacts directly and throughout supply chains.

Historically, transportation companies have been more focused on safety and physical security than cybersecurity. As technological advancements have created the ability and the need to be ever more connected, that paradigm is changing. Cybercriminals are aware of the critical nature of transportation and will continue to maliciously exploit vulnerabilities to achieve their goals. Between June 2020 and June 2021, according to some reports, the transportation industry witnessed a 186 percent increase in weekly ransomware attacks.[53]

TSA's new cybersecurity requirements will help keep the surface transportation systems and associated infrastructure secure and protect our critical infrastructure from evolving cybersecurity threats. TSA's performance-based regulation provides owner/operators the

---

[52] U.S. Department of Transportation. Bureau of Transportation Statistics, Freight Facts and Figures. 2022. Moving Goods in the United States. https://data.bts.gov/stories/s/Moving-Goods-in-the-United-States/bcyt-rqmu. Accessed July 5, 2023.

[53] Bowcut, Steven. Jun. 5, 2023. "Cybersecurity in the transportation industry." Cybersecurity Guide. https://cybersecurityguide.org/industries/transportation/. Accessed July 5, 2023.

flexibility to determine how to implement cybersecurity protocols to achieve the desired outcomes. Such flexibilities can include broad items, such as monitoring, which can evolve as related technology develops or be tailored to a specific owner/operator versus a prescriptive requirement. Another example of this flexibility is patch management, whereby not having a prescriptive requirement, owner/operators can evaluate and rank risk factors, understand impacts, and then determine or prioritize deployment. Additionally, affected owner/operators can adapt their processes and systems to any requirements promulgated by state, local, or federal governments. For instance, the Federal Transit Administration has a program where recipients have to follow several requirements in the cyber space as a condition of being awarded the grant.[54] The flexibility to choose how to achieve performance objectives allows for owners/operators to be more innovative and work towards improving their plans and processes based on the best method for them to meet the needed criteria set forth in requirements. Given the rapid pace of innovation and evolution in technology, and the associated increased risk of a cyber-attack, these requirements will enable owners/operators to build and maintain a stalwart defense and be able to proactively mitigate system vulnerabilities. Designating a cybersecurity coordinator will enable information sharing between the government and owner/operators, reporting cybersecurity incidents enables CISA and TSA to provide knowledge and assistance when there are cyber-incidents. A well-defined CRM program will ensure that systems are reviewed and maintained and staff is appropriately trained while giving owners/operators the performance-based flexibility to make decisions suitable for their industry and workplace. Given the increased frequency and potential severity of cybersecurity incidents, TSA has determined

[54] Per the Federal Transit Administration, as a condition of Federal assistance, under 49 U.S.C. 5323(v), rail transit operators must certify that they have a process to develop, maintain, and execute a plan for identifying and reducing cybersecurity risks.

the provisions detailed in this rule are both necessary and appropriate.

1.2 Market Failure

The threat of a cyber-attack on the surface transportation systems and associated infrastructure is real. However, due to the economics of externalities, the market for surface transportation may not provide adequate incentives for entities in these industries to make socially optimal[55] investments in the full range of measures that would reduce the probability of a successful cyber-attack or its impact on society.

Externalities are costs or benefits from an economic transaction experienced by parties external to the transaction. In the case of surface transportation, the total consequences of a cyber-attack, or other security incident, may be significantly greater than what would be realized by an individual owner/operator. For instance, should a passenger rail train be taken off line, riders would experience delays, potentially need to find alternate methods of transportation, and it may result in increased traffic on roads or rescheduling of business engagements. As a real world example, in March 2023, a nationwide outage of Positive Train Control (PTC) for Amtrak resulted in cancelled and delayed trains in and out of Chicago for multiple days, affecting Amtrak, commuter railroads, and freight railroads [56] As a result, the private market may not provide sufficient incentive for profit-maximizing firms to unilaterally spend the socially optimal amount of resources to prevent or mitigate an attack. The government is able to use its authority through the rulemaking process to set forth minimum obligations to which affected

[55] For purposes of this analysis, a socially optimal result relates to the ideal distribution of all resources in a society while accounting for internal and external benefits and costs.

[56] *See* Johnson, *PTC issues cause Amtrak cancellations and delays*, Trains.com (posted Mar. 24, 2023), available at https://www.trains.com/trn/news-reviews/news-wire/ptc-issues-cause-amtrak-cancellations-and-delays/ (last accessed Nov. 28, 2023).

owner/operators must adhere when necessary. TSA believes that the compounding damage of a successful cyber attack could be so vast that it would result in an impact to society at large, well beyond the profit maximizing priorities of an individual company. Additionally, this proposed rulemaking is needed as one effect of market failure is the inefficient allocation of resources. Individual companies may see investing in cybersecurity measures as inefficient as individuals or society who are not directly tied to said company would receive benefits in terms of increased security. All affected entities—except for public transportation agencies—are privately owned and are susceptible to externalities that would provide an incentive preventing them from spending the socially optimal amount on cybersecurity. Public transportation agencies face similar market forces as privately owned companies and face many demands for limited ridership revenues and tax dollars.

Many companies have limited resources available and competing priorities to manage risk. When it comes to cybersecurity where threats and technology evolve rapidly, it can be challenging to determine where and how to make investments. The presence of uncertainty, in not being able to know when or how an attack might occur (or its probability) and different risk tolerances, adds an additional level of complexity for companies determining which cybersecurity methods to implement and to what extent. As a result, owner/operators have invested resources in implementing cybersecurity measures to varying degrees. For example, TSA points to efforts undertaken by the Communications Security, Reliability, and Interoperability Council (CSRIC), which provides recommendations to the FCC to "address the

prevention and remediation of detrimental cybersecurity events."[57] CSRIC Working Group #7 developed the Anti-Bot Code of Conduct (ABC) for ISPs which was released in March 2012 as a cooperative industry-government initiative. Following the adoption, the FCC received commitments from a number of ISPs to implement the ABC as a way to demonstrate a commitment to working against bots and malware. These ABCs include activities related to education, detection, notification, remediation, and collaboration.[58] However, as companies are operating with limited capacity to evaluate threats and technological solutions, such investment is likely to be inconsistent and varies across the industry. Companies willing to accept a higher amount of risk may choose to devote fewer resources to cybersecurity threat prevention, response, or mitigation. This is additionally hampered by the fact that as there is no one-size-fits-all standard or requirement that all entities are working towards. While NIST, for example, includes specific measures, it is voluntary and there remains differences across companies in what are key items to be addressed, equipment being used, processes employed, and how security measures are implemented and to what extent, given budgetary constraints and levels of maturity. Further, in a competitive marketplace, a firm normally will not choose to make additional investment in cybersecurity over its privately optimal amount, since such an investment would increase the firm's cost of operation, placing it at a disadvantage when competing with companies that have not chosen to make a similar investment in cybersecurity.

[57] For an overview on the purpose and focus of the CSRIC, see the CSRIC page, available at https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-0. Accessed August 26, 2024.

[58] For the Code of Conduct and additional discussion of the activity areas, see the ABCs for ISPs page, available at https://www.m3aawg.org/abcs-for-ISP-code. Accessed August 26, 2024.

1.3 Need for Regulatory Action

Transportation of people and goods plays a critical role in the national economy and American way of life. Pipeline and rail owner/operators[59] in many cases continue to advance and increase interconnectedness of OT[60] and IT[61] systems. Such developments provide many efficiencies (e.g., increased automation and remote access) but also poses risk and potential vulnerabilities to new and evolving cyber threats. The increasing integration of IT, connectivity to the internet, and the ability to perform tasks remotely have revolutionized the transportation industry. However, these advancements may have also exposed transportation companies to new cybersecurity risks. Given the critical role transportation plays in our economy, national security, and public well-being, it is imperative to prioritize cybersecurity.

As discussed in Section 1.2, companies are managing competing priorities with finite resources. With the uncertainty surrounding future technological innovation and the corresponding threat evolution, there is an additional layer of complexity added to the analysis of building a cybersecurity defense. Given the ever present threat of cybersecurity attacks and the potential economic and societal consequences, TSA believes there is a need for this regulation.

A successfully cyber-attack could result in real world negative consequences. For example, a

---

[59] *See* definition of "owner/operator" in 49 CFR 1500.3.

[60] For purposes of this proposed rule, 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 (SCADA) 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."

[61] For purposes of this proposed rule, 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."

successful cyber-intrusion affecting OT systems could impact industrial control systems (ICS) including SCADA systems, process control systems, distributed control systems, measurement systems, and telemetry systems which could impact the ability for companies to safely operate their systems. More recently, in December 2020, a highly sophisticated attack was discovered, targeting SolarWinds, an IT management software provider. The attack compromised SolarWinds' software, leading to the distribution of a malware-infected update to their Orion platform.[62] This attack impacted numerous organizations and government agencies, including the U.S. Department of Defense and DHS. As CISA has noted, recent cybersecurity incidents demonstrate that intrusions affecting IT systems can also affect critical operational processes even if the intrusion does not directly impact OT systems.[63]

As technology continues to advance and become interconnected with our daily lives, so too does the incident risk in terms of possible vulnerability points and levels of impact. In 2023 CISA issued advisories for 49 vulnerabilities in eight industrial control systems (ICS) utilized across multiple critical infrastructure sectors (including the transportation sector), noting that some are unpatched. As detailed in an article on Dark Reading, ICS and OT environments are no longer air-gapped, segmented as they once used to be, and are increasingly accessible over the internet, resulting in those networks being increasingly popular targets for both nation-state actors and financially motivated threat groups. The vulnerabilities cited in the CISA advisory can allow

---

[62] See Martínez, J., & Durán, J. N. (2021). Software Supply Chain Attacks, a Threat to Global Cybersecurity: SolarWinds' Case Study. International Journal of Safety and Security Engineering, 11(5), 537–545. https://doi.org/10.18280/ijsse.110505 and Peisert, S., Schneier, B., Okhravi, H., Massacci, F., Benzel, T., Landwehr, C. E., Mannan, M., Mirkovic, J., Prakash, A., & Michael, J. B. (2021). Perspectives on the SolarWinds Incident. IEEE Security & Privacy, 19(2), 7–13. https://doi.org/10.1109/msec.2021.3051235

[63] *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.

attackers to "take control of affected systems, manipulate and modify settings, escalate privileges, bypass security controls, steal data, and crash systems."[64] A report from Armis, an asset intelligence cybersecurity company, found that global attack attempts more than doubled in 2023.[65] The report also found that "cybersecurity blind spots and critical vulnerabilities are worsening". Such increase could impact the transportation industry. For example, the Greater Richmond Transit company had its network impacted in November 2023 which followed a string of public transit system-targeted intrusions that has been ongoing since 2021, including an October 2023 incident occurring at Metro Call-A-Ride in St. Louis, Missouri.[66]

Given the world's increasing reliance on IT, the resulting impact of a cybersecurity issue can have a domino effect. While not caused by a cybersecurity attack, an incident with a CrowdStrike update that was pushed out to clients caused systems to go offline, resulting in impacts felt across industries including systems issues at hospitals and banks, grounding of flights, and impacts to transit systems as well as federal, state, and local government systems, among others.[67] In the days following the issue, CrowdStrike warned about the potential for, and reports of, bad actors capitalizing on the event in order to engage in "malicious" activity,

---

[64] *See* CISA Warns on Unpatched ICS Vulnerabilities Lurking in Critical Infrastructure (March 2023), available at https://www.darkreading.com/vulnerabilities-threats/cisa-warns-unpatched-vulnerabilities-ics-critical-infrastructure. Accessed July 27, 2024.

[65] *See* Cybersecurity Attack Attempts More Than Doubled, Increasing 104% in 2023 (January 2024), available at https://apnews.com/press-release/business-wire/california-165f1a4a3b5e44d0bc0414f4012ef74c. Accessed July 27, 2024

[66] *See* Cyberattack hits Central Virginia transit system (December 11, 2023), available at https://www.scmagazine.com/brief/cyberattack-hits-central-virginia-transit-system. Accessed July 27, 2024

[67] *See* CrowdStrike outage sparks global chaos with airline, bank and other disruptions (July 2024). Available at https://www.msn.com/en-us/money/companies/crowdstrike-outage-sparks-global-chaos-with-airline-bank-and-other-disruptions/ar-BB1qg2I0?ocid=BingNewsSerp. Accessed July 27, 2024

including sending phishing emails and trying to sell scripts that claim to fix the issues.68 This further underscores the need for strong cybersecurity systems and processes as even when unintentional incidents happen (not due to a cyberattack), there are real world ramifications and the potential for more insidious behavior.

Therefore, TSA is proposing regulatory action to develop a CRM system requiring regulated parties to appoint a cybersecurity coordinator, report cybersecurity incidents, and develop a comprehensive cybersecurity risk management program thereby addressing the threat posed by cyber-attacks and inconsistent levels of cybersecurity protection across industry.[69] By structuring the requirements from a performance focus, rather than prescriptive, covered owner/operators maintain the flexibilities needed to account for differences in business operations and the evolving cyber environment while still establishing benchmark and uniform guidelines that raise cybersecurity prominence when competing with other priorities and foster continual cybersecurity across the full industries.[70] For instance, a Cybersecurity Evaluation would require owner/operators to identify cybersecurity vulnerabilities as well as areas where readiness could be strengthened. Then, measures undertaken as part of COIP development, such as identifying critical cybersecurity systems, protection of critical systems, and having procedures, policies, and capabilities to respond to and recover from cyber incidents would, among other things,

---

[68] *See* Falcon Sensor Content Issue from July 19, 2024, Likely Used to Target CrowdStrike Customers (July 19, 2024), available at https://www.crowdstrike.com/blog/falcon-sensor-issue-use-to-target-crowdstrike-customers/. Accessed July 27, 2024

[69] TSA recognizes that some entities may have already take cybersecurity actions that address the needs identified; however, based on insight from SD owner/operator self assessments and industry engagement, it does not appear as though industry is sufficiently implementing preventative measures on its own or consistently across the industry.

[70] TSA notes that entities can leverage existing cybersecurity efforts to satisfy regulatory requirements; but for those who are not, or not to a sufficient degree, would increase such efforts and reap the associated benefits.

encourage owner/operators to identify which systems need higher levels of protection, implement protection measures (e.g. control points of access), and have measures in place to address an intrusion or incident. Finally, an entities CAP would encourage evaluation of one's efforts over time and foster continual improvement. Specific discussion on how various elements can help address the issues identified above can be found in Section 4.1. Ultimately, transportation companies can help protect critical infrastructure, maintain economic stability, and ensure the safe and reliable movement of goods and people by implementing new cybersecurity requirements and adopting robust security measures.

1.4 Statutory Authority

The Aviation and Transportation Security Act, Pub. L. 107-71, 115 Stat. 597 (November 19, 2001), gives TSA broad responsibility and authority for "security in all modes of transportation" including aviation and "other modes of transportation that are exercised by the Department of Transportation." *See* 49 U.S.C. 114(d). In addition, as part of the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Act), Congress enacted requirements related to protection of certain critical pipelines, freight rail carriers, public transit passenger railroad (PTPR), and Over-the-Road Bus (OTRB) entities. This proposed rule is consistent with TSA's mission, as well as TSA's responsibility and authority identified above.

TSA, under this authority, can establish regulations to enhance the cybersecurity posture of regulated entities. TSA, following input from CISA, Department of Transportation (including the Federal Railroad Administration, Pipeline and Hazardous Materials Safety Administration, and the Federal Transit Administration), the Federal Energy Regulatory Commission (FERC), the Department of Energy, the United States Coast Guard, and consultation with industry stakeholders proposes this rulemaking to enhance the cybersecurity posture of surface modes and

meet aspects of its statutory obligations under the 9/11 Act. The required cybersecurity measures provide covered entities with an improved ability to prevent cyber-attacks, mitigate the damage from a cyber-attack, and more quickly recover from a cyber-attack. The benefits related to these outcomes are further discussed in Section 4.

1.5 Advance Notice of Proposed Rulemaking (ANPRM) Comment Discussion

TSA received several dozen public comments to the Enhancing Surface Cyber Risk Management ANPRM. A wide variety of interested parties provided these comments, including pipeline and railroad entities, industry associations (including an airline association), a labor union, third-party vendors (TPVs), and private individuals. TSA appreciates the input from the public, and took said comments into account, as appropriate, when drafting the notice of proposed rulemaking (NPRM). The following summarizes key points from comments received that related to the economic impact of the proposed rulemaking as well as TSA response.

First, commenters expressed the need for flexibility in the requirements of the rule to address the evolving cybersecurity threat landscape and to allow for variations between industry needs.[71] Commenters also indicated that an owner/operator's approach to CRM implementation is based on many factors, such as the organization's size, diversity of operations, cybersecurity maturity, overall risk tolerance, and available resources, among others. TSA acknowledges such circumstances and has thus developed a risk- and performance-based approach to CRM program implementation that will enable owner/operators to develop their own plans for mitigating the risks associated with cybersecurity incidents.

[71] Crowd Strike (TSA-2022-0001-0010); PJM Interconnection, LLC (TSA-2022-0001-0033); American Fuel & Petrochemical Manufacturers (AFPM) (TSA-2022-0001-0035); American Public Gas Association (APGA) (TSA-2022-0001-0029); Colonial Pipeline Company (TSA-2022-0001-0023).

Beyond the different cybersecurity measures an owner/operator can implement, commenters also discussed the wide range of cybersecurity incidents, severity of business disruptions, and the need for restoration of operations as factors that impact the range of cybersecurity incident cost estimates.[72] Therefore, quantification of costs associated with CRM programs can be challenging given the wide range of parameters that influence the estimation. TSA received specific comments asking that it consider scalability in its rulemaking, and to avoid a one-size-fits-all approach.[73] Again, TSA has developed a performance-based approach that will allow affected entities to meet the requirements in ways that make sense for them, so long as the benchmarks discussed in the preamble are met, rather than prescriptive requirements.

Several commenters noted that likely covered entities already have many cybersecurity protections in place, and that TSA should take these baseline efforts into account as cybersecurity protections are expensive.[74] TSA acknowledges that many organizations already implement CRM programs to some degree; however, TSA also notes there may be disparities between the CRM program maturity due to resourcing and workforce issues. However, because such efforts may have been done on a voluntary basis to the extent that companies were not mandated to implement specific actions prior to the SDs and could, theoretically, cease implementation, and because actions related to the SDs were employed prior to this rule, this analysis attempts to capture the full cost of its regulatory requirements without specifically

[72] NiSource Inc. (TSA-2022-0001-0019); American Fuel & Petrochemical Manufacturers (AFPM) (TSA-2022-0001-0035)

[73] American Fuel & Petrochemical Manufacturers (AFPM) (TSA-2022-0001-0035); Liquid Energy Pipeline Association (TSA-2022-0001-0014); American Public Gas Association (APGA) (TSA-2022-0001-0029).

[74] American Gas Association (TSA-2022-0001-0021); New Mexico Gas Company (TSA-2022-0001-0016); NiSource Inc. (TSA-2022-0001-0019); Pacific Gas and Electric Company (TSA-2022-0001-0028); Exelon Corporation (TSA-2022-0001-0031).

quantifying previous industry actions including those before or after the issuance of the SDs. Nonetheless, TSA also appreciates that the costs will vary across each owner/operator, and thus has included a qualitative discussion of possible ranges for proposed provisions when appropriate to enhance the quantified point estimates of incurred costs. In addition, TSA also includes a sensitivity analysis of identified key cost drivers.

Throughout the ANPRM, TSA posed queries and sought feedback from industry organizations and the public regarding elements of a potential CRM rule that have the potential to greatly impact implementation costs, such as workforce concerns, the use third-party vendors, and potential required technology, among others. In response, a number of commenters expressed concerns over the lack of available resources to fund potential CRM program elements and how an organization's size and complexity greatly affect the number of cyber-trained staff needed to effectively implement CRM. One commenter was specifically concerned about the need to hire and train additional cybersecurity staff, noting that cybersecurity professionals are a high-demand, low-supply asset.[75] Another commenter noted that the cybersecurity coordinator would likely be multiple people at large organizations.[76] TSA recognizes there are costs associated with improving cybersecurity. TSA notes that the NPRM does not mandate the hiring of additional personnel to comply with the proposed rule and that many of the provisions incorporate flexibility to allow companies to develop methods that work best for themselves and within their available resources and improve over time. Comments were also received suggesting that TSA consider offsetting costs or incentivizing covered industries. Some commenters urged TSA to

[75] Interstate Natural Gas Association of America (INGAA) (TSA-2022-0001-0024)
[76] Individual (TSA-2022-0001-0003).

offer grants[77] while another proposed that TSA establish a refundable account to businesses, similar to the refundable accounts the Federal Energy Regulatory Commission (FERC) offers.[78] TSA acknowledges that while funding support through means such as grants or compliance incentives has the potential to reduce the overall burden of CRM program implementation on industry, such funding would not change the overall cost of the rule and such funding mechanisms coming directly from TSA are not available.[79] However, there may be some existing grant programs available that affected owner/operators may pursue. As an example, CISA has a State and Local Cybersecurity grant program that helps eligible entities address cybersecurity risks and threats to information systems owned or operated by – on behalf of – state, local, and territorial governments.[80] In addition, DHS administers a Transit Security Grant Program that provides funding to eligible public transportation systems (which include intra-city bus, ferries and all forms of passenger rail) to protect critical transportation infrastructure and the travelling public from terrorism, and to increase transportation infrastructure resilience.[81] This cost analysis does not anticipate the acquisition of any grants by any affected owner/operators.

In addition, commenters recommended TSA align its cybersecurity requirements with those of other agencies responsible for oversight of critical infrastructure. Some commenters mentioned

---

[77] Individual (TSA-2022-0001-0003); American Gas Association (TSA-2022-0001-0021); Exelon Corporation (TSA-2022-0001-0031).

[78] Southern California Gas Company ("SoCalGas") and San Diego Gas and Electric Company ("SDG&E") (TSA-2022-0001-0034).

[79] TSA does not guarantee that stakeholder participation in TSA's structured oversight initiatives will result in a grant award or determination of applicability eligibility, however utilization of a Baseline Assessments for Security Enhancement (BASE) security assessment or Transportation Security Template and Assessment Review Toolkit (T-START) to build a security system security plan have historically helped applicants to meet the criteria for some baseline requirements for certain applicable FEMA Preparedness Grants related to surface transportation.

[80] Further information can be found at the grant program website, https://www.cisa.gov/state-and-local-cybersecurity-grant-program

[81] Further information can be found at the grant program website, https://www.fema.gov/grants/preparedness/transit-security.

current rulemaking efforts by CISA, and expressed concern about overlapping compliance obligations. One commenter recommended rather than creating new cybersecurity standards, adopting related standards already proposed by the Federal Energy Regulatory Commission (FERC) and the Department of Defense. TSA acknowledges commenters' concerns over the need for harmonization between existing cybersecurity regulations as new requirements may result in additional burdens for organizations affected by the rule. TSA appreciates this concern and is working with other agencies, including those that are in DHS, to minimize duplication of requirements and ensure there are not issues related to regulatory overlap.

There was some broad concern that the focus of the rule should not be too restrictive. A business association stated that mandating security controls assumes that threats and technologies will not adapt to changing landscapes, and it may not be effective in all environments.[82] The commenter recommended that the focus should be on achieving outcomes or performance goals that suit the different security operations. Another commenter recommended TSA and CISA collaborate to create cohesion on performance goals such as incident reporting, while another suggested TSA collaborate with another agency on Cybersecurity Implementation Plan (CIP) and not approve CIPs alone.[83] TSA concurs with the point of technology and threats evolving and the need for flexibility. The rule is structured in a way to provide such flexibility to owner/operators and focuses on outcomes to be achieved from a performance focus versus a prescriptive one.

Finally, several comments address IT and OT penetration testing, with some commenters recommending the use of third party vendors (TPVs) to assist with this requirement, while other

[82] Interstate Natural Gas Association of America (INGAA) (TSA-2022-0001-0024).
[83] American Petroleum Institute (API) (TSA-2022-0001-0027); Individual (TSA-2022-0001-0003).

commenters were opposed. As noted above, TSA has designed this rule in a way where owner/operators are able to achieve compliance in ways that make the most sense for them across the provisions, which can include utilizing TPVs, and including how penetration testing could be used as an assessment capability along with other capabilities such as red/purple team testing.

Regarding benefits, one commenter said that the requirement to conduct a cybersecurity vulnerability assessment will help entities identify and remediate perceived threats while some questioned the benefits of potentially requiring accredited third party audits/assessments to determine the effectiveness of the owner/operator's cybersecurity measures and/or compliance with existing measures.[84] Although most likely agree that there is benefit to improved cybersecurity, TSA understands there may be some skepticism among stakeholders, especially regarding the potential benefits of specific provisions. TSA notes that this NPRM does not require third-party audits or assessments, but that such actions are performed by independent assessors. In addition, in the benefits section, TSA articulates how each provision is expected to yield benefits. TSA also presents a break-even analysis that details how benefits can be derived from preventing cybersecurity incidents across a variety of scenarios.

1.6 Requirements of the Proposed Rule

There is a real and ongoing threat of a cyber-attack, whether from cyberterrorists or cybercriminals, against pipeline, freight rail, or passenger transit users, employees, facilities, and infrastructure, as well as the use of surface transportation modes as a conduit for terrorist attacks

[84] Colonial Pipeline Company (TSA-2022-0001-0023); Southern California Gas Company ("SoCalGas") and San Diego Gas and Electric Company ("SDG&E") (TSA-2022-0001-0034).

on American soil. A cyber-attack against surface transportation modes could disable or disrupt transportation of products (pipelines/freight rail), services (passenger transit), or both, inflicting a significant economic impact on a city, region, or nation. TSA issued security directives in 2021, 2022, and 2023[85] 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."[86]

In an attempt to mitigate the risk of a cyber-attack, the proposed rule contains a number of requirements for owner/operators to develop a cybersecurity risk management program that would help prevent cyber-attacks, mitigate the damage from a cyber-attack, and allow a company to more quickly recover from a cyber-attack. The proposed rule incorporates the requirements of TSA's previous cybersecurity security directives described above and expands upon them where warranted. Specifically, the rule includes provisions relating to designating an accountable executive and cybersecurity coordinator, reporting incidents to CISA, developing and maintaining cybersecurity incident response and implementation plans, conducting a cybersecurity evaluation and assessment, and training for applicable employees, along with appropriate recordkeeping and compliance requirements. Table 1-1 presents each of the proposed

---

[85] *See* https://www.tsa.gov/for-industry/surface-transportation-cybersecurity-toolkit for links to the SDs. TSA issued these security directives under the specific authority of 49 U.S.C. 114(*l*)(2)(A). 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 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.

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

rule's requirements.

Table 1-1: Affected Population by Mode and CRM Requirement

Requirement	Freight Rail	PTPR	OTRB	Pipeline
Cybersecurity Evaluation (CSE)	✓	✓		✓
Cybersecurity Operational Implementation Plan (COIP)	✓	✓		✓
Accountable Executive	✓	✓		✓
Cybersecurity Coordinator	✓	✓		✓
Training	✓	✓		✓
Reporting Cybersecurity Incidents to CISA	✓	✓	✓	✓
Cybersecurity Incident Response Plan (CIRP)	✓	✓		✓
Cybersecurity Assessment Plan (CAP)	✓	✓		✓

These requirements would persist over time and include various, at times sequential, and often multiple submissions tied to updates and regular reviews that foster continuous improvement as an owner/operator's cybersecurity posture improves as part of the iterative process required by the proposed rule.[87] Implementation timelines will vary by owner/operator and by many entities who have already taken actions through SDs. Nonetheless, TSA estimates that the full iterative cycle would take approximately four years, moving from Cybersecurity Evaluation, COIP development, COIP implementation, CAP implementation (which includes a three-year plan for assessing all of the COIP and Critical Cyber Systems, annual CAP Reports, and changes to the COIP based on the CAP Report and annual Cybersecurity Evaluations. Specifically, an entity would complete a number of requirements in Year 1 including development and implementation of their COIP. They would then begin their CAP development (following COIP approval). The

[87] Development of some elements are predicated on the development and approval of others. For instance, one's COIP needs to be implemented before beginning the processes related to the CAP and CAP report, which assesses and tests the COIP.

CAP then requires at least one-third of processes be evaluated each year, aggregating up to a minimum of 100 percent evaluation over a three-year period. However, TSA also notes that Table 7 in Section H of the NPRM provides details on compliance deadlines and documentation based on how submissions relate to current SD efforts.

1.7 Baseline Summary

The baseline summary presents a brief description of each impacted industry and represents TSA's best assessment of what the world would be like absent this regulatory action.[88]

In general, there are a number of cybersecurity standards available as a resource for owners/operators across industry. However, implementation of such standards is not required and it is up to individual companies to choose which recommendations to implement and their level of implementation and maintenance of cybersecurity measures. For example, the National Institute of Standards and Technology (NIST) provides an organizing framework to establish cybersecurity standards. The Cybersecurity Framework from NIST details the 5 current pillars of focus: Identify, Protect, Detect, Respond, Recover.[89] There are a variety of other standards or guidance with a cybersecurity focus that owner/operators have likely considered, including from other federal agencies; however, TSA does not have comprehensive data regarding usage and adherence.[90]

TSA also recently issued security directives (SD) in 2021, 2022, and 2023 in response to

---

[88] Office of Information and Regulatory Affairs, "Regulatory Impact Analysis: A Primer," August 15, 2011, pg. 4 https://www.reginfo.gov/public/jsp/Utilities/circular-a-4_regulatory-impact-analysis-a-primer.pdf. Accessed on May 17, 2022.

[89] For more information, see the NIST Cybersecurity Framework at https://www.nist.gov/cyberframework. Note that the framework is in the process of being updated and this RIA references Version 1.1 of the framework.

[90] A discussion of standards can be found in the NIST publication Cyber Security Standards, available at https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=152153.

cybersecurity risks to designated freight railroads, passenger rail and rail transit owner/operators, and pipeline owner/operators, the specifics of which are provided below. 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 measures.[91]

As a result of the publication of TSA's cybersecurity SDs, as well as prior industry actions and best practices, many owner/operators already employ measures that would satisfy some of the proposed rule's requirements. As such, owner/operators have already incurred costs, and in some cases significant costs, especially to address cybersecurity concerns and ensure compliance with SD requirements.

However, given the recency of the SDs and voluntary nature of previous industry cybersecurity efforts prior to the SDs with no specific actions or requirements previously included in regulation, TSA uses a zero baseline that evaluates all requirements as new and thus provides an assessment of the impact of the full CRM program. Assuming a baseline level of compliance as zero ensures TSA captures all of the costs related to the requirements of this rulemaking. Furthermore, costs were not provided as part of the SDs' publication, and the SDs will be rescinded upon publication of a final CRM rule; thus, this economic analysis endeavors to account for the full cost of the cybersecurity provisions set out by TSA.

While cybersecurity is not a novel undertaking for companies, TSA has not included a separate baseline accounting for current industry cybersecurity practices in part due to the lack of information and metrics on such practices and wide range of entity processes and systems

[91] *See* Information Circular: Surface Transportation IC-2021-01: Enhancing Surface Transportation Cybersecurity at https://www.tsa.gov/sites/default/files/20211201_surface-ic-2021-01.pdf. Accessed on Oct. 19, 2022.

maturity. However, TSA notes that potential costs and benefits of this proposed rule should be interpreted in light of the baseline as well. To the extent that some percentage of companies are already implementing adequate cyber security policies consistent with the guidelines described in this rulemaking, the proposed marginal costs and benefits would not accrue to those companies.

In addition, while many of the provisions in this NPRM are carried over from the SDs, their recent publication means that they have not been in place long enough for owner/operators to reach full implementation. Furthermore, any information provided to TSA by covered entities regarding specific levels of compliance with the SD requirements is considered Sensitive Security Information (SSI).

Nonetheless, TSA requests public comment on the degree to which requirements have already been implemented including any associated cost information.

The cost of complying with the CRM requirements for a specific entity depends on the entity's specifics needs and the extent that company is already undertaking some of the required actions. For instance, if an owner/operator already had a designated cybersecurity coordinator, then that provision of the rule wouldn't cost that entity any more than it was already incurring. If a second entity designated a cybersecurity coordinator because of TSA's cybersecurity SD, then it too would have already incurred the associated cost. However, as discussed above, to fully account for the rule's cost relative to existing regulatory requirements, TSA includes these costs in both instances plus any additional owner/operators who designate a cybersecurity coordinator as a result of the rule. On the other hand, TSA does, where possible, identify instances, and qualitatively discusses, costs that owner/operators may have already incurred to provide

additional context of the rule's incremental costs. In addition, TSA generally portrays an average or typical entity cost to reflect the overall cost of the rule that doesn't provide an exact accounting for individual entities.

In addition, TSA has also developed a sensitivity analysis in Section 3.8 that considers the uncertainty related to the largest cost drivers: access control, critical cyber systems data backup, and cybersecurity training. This analysis captures both uncertainties related to existing implementation as well as uncertainty with how owner/operators will achieve the performance based metrics.

1.7.1 Security Directive to Rule Comparison

The differences between SD applicability and the applicability of the rule reflect that SDs are intended to be limited term requirements directed at those entities most at risk to a specific threat while regulations are intended to be long-term. In this case the proposed regulation would mandate performance-based cyber risk management requirements that address current cybersecurity risks, while maintaining the flexibility necessary to address emerging threats and deploy evolving capabilities. The TSA-issued cybersecurity SDs targeted a specific group of rail and pipeline owner/operators: for rail, TSA utilized pre-existing regulatory categories that encompassed the rail carriers TSA intended to include. For pipeline, TSA utilized a pre-existing list of owner/operators that have been designated as critical by TSA for purposes of the assessment required by the 9/11 Act and are covered parties under current TSA Pipeline Security Directives. In thinking about the longer-term requirements in a regulation, TSA used the aforementioned regulatory categories and the TSA-designated critical list as the base applicability for a cyber risk management rulemaking. TSA concluded to best protect the greatest number of passengers and the supply chain that supports national and economic security,

the rule should incorporate additional rail carriers and pipeline facility or systems owner/operators that moved the greatest volume of cargo, people, or hazardous liquids or natural gas or supply other critical infrastructure sectors, for example the Department of Defense. Table 1-2 shows how the number of covered entities within each industry changed as guidance evolved.

Table 1-2: Number of Covered Entities in the Security Directives Information Circulars and Rule

Published Notice	Effective Date	Freight Railroad	PTPR	OTRB	Pipeline
SD Pipeline-2021-01	May 28, 2021				100
SD Pipeline-2021-02	July 26, 2021				100
SD Pipeline-2021-01A	December 1, 2021				96
SD Pipeline-2021-02B	December 17, 2021				96
SD 1580-21-01	December 31, 2021	62			
SD 1582-21-01	December 31, 2021		31		
ST IC-2021-01	December 31, 2021	395	84	71	0
IC Pipeline-2022-01	February 16, 2022				2900
ST IC-2022-01	February 25, 2022	395	84	71	0
ST IC-2022-02	March 23, 2022	395	84	71	2900
SD Pipeline-2021-01B	May 29, 2022				96
SD Pipeline-2021-02C	July 27, 2022				96
SD 1580-21-01A	October 24, 2022	62			
SD 1582-21-01A	October 24, 2022	0	31		
SD 1580/82-2022-01	October 24, 2022	62	5		
SD Pipeline-2021-01C	May 29, 2023				91
SD Pipeline-2021-02D	July 27, 2023				91
NPRM	TBD	73	34	71	115

This proposed rule builds upon previously issued Security Directives which many of the affected owner/operators have endeavored to implement. All the SD requirements have been carried over, either in full or with minor alteration, to the NPRM. New requirements include cybersecurity reporting for the OTRB industry; specific requirements for governance of the CRM programs; supply chain risk management requirements addressed as part of the COIP; and cybersecurity training. This proposed rulemaking also adds in physical security requirements for the covered pipeline industry, but those provisions are not considered part of the CRM program. A summary of key updates is listed below, and a more comprehensive table can be found in Appendix A:

- Cybersecurity Evaluation – 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. This requirement is also consistent with recommendations in the NIST Cybersecurity Framework and CISA's CPGs. The process to develop this profile is substantively similar to the requirements laid out in the applicable SDs.
- Cybersecurity Operational Implementation Plan (COIP) – 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 Cybersecurity Implementation Plan. 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 Plan of Action and Milestones (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 – Consistent with TSA's intent to align the requirements in the rule with the NIST Cybersecurity Framework, 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 by providing structure, roles, and encouraging cybersecurity as an organizational goal. The "governance" requirements

include designation of the accountable executive responsible for planning, resourcing, and execution of cybersecurity activities.

- Cybersecurity Coordinator – 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, and having a Homeland Security Information Network (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 recognizes the distinction between physical security and cybersecurity and the possibility that organizations may need to have different individuals handling these responsibilities.
- Identification of Critical Cyber Systems – 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.
- Supply Chain Risk Management – 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 – 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 Cybersecurity Framework.
- Cybersecurity Training – TSA is proposing a new requirement for cybersecurity training for basic users as well as role-based cybersecurity training for privileged users. This proposed requirement is consistent with recommendations in CISA's CPGS.
- Detection of Cybersecurity Incidents – 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 Cybersecurity Framework.
- Capabilities to Respond to a Cybersecurity Incident – 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 Cybersecurity Framework.
- Cybersecurity Incident Reporting – 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) – 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 which must also include exercises. The CIRP requirements in the proposed rule are substantively the same as in the SDs but with some language changes.
- Cybersecurity Assessment Plan (CAP) – 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 and its identified measures. As laid out in the applicable SDs, consistent with the NIST Cybersecurity Framework, 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.

1.7.2 Freight

The national freight rail network is a complex system that includes both physical and cyber infrastructure and consists of nearly 140,000 rail miles operated by six Class I railroads, 580 local (also known as Short Line) railroads, and 21 regional railroads. Each Class I railroad had operating revenues of at least $900 million in 2021. 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.[92] As stated by the

[92] Association of American Railroads (AAR). Jun. 2023. Railroad 101. https://www.aar.org/wp-content/uploads/2020/08/AAR-Railroad-101-Freight-Railroads-Fact-Sheet.pdf. Accessed on Oct. 19, 2022.

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."[93] Freight railroads are private entities which own and are responsible for their own infrastructure. 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, freight railroads are subject to safety regulations put forth and enforced by the Federal Railroad Administration (FRA). TSA administers and enforces rail security regulations contained in 49 CFR part 1580. For purposes of this analysis, TSA is estimating that 25 of the 73 freight owner/operators affected by the proposed rule will be small entities, as designated by the Small Business Administration (SBA) size class standards.[94]

As discussed previously, TSA assesses all the proposed rule requirements as new and presents a baseline level of compliance of zero. However, TSA recognizes that owner/operators may have started implementing a cybersecurity risk management program previously, including actions related to TSA issued SDs to higher-risk freight railroads in December 2021 (the SD 1580-21-01 series) that include: (1) designation of a cybersecurity coordinator and alternate; (2) reporting of cybersecurity incidents to CISA within 24 hours; (3) developing and implementing a CIRP to reduce the risk of an operational disruption; and (4) completing a cybersecurity vulnerability assessment to identify potential gaps or vulnerabilities in their systems. TSA also issued an "information circular" (IC-2021-01), which included a non-binding recommendation for those

[93] *Id.*
[94] SBA. Table of Small Business Size Standards Matched to North American Industry Classification System Codes. https://www.sba.gov/sites/default/files/files/Size_Standards_Table_2022.pdf. Effective May 2, 2022.

surface owner/operators not subject to the SDs to voluntarily implement the same measures.[95] On October 18, 2022, TSA issued a SD imposing performance-based cybersecurity requirements on higher-risk freight railroads, passenger rail, and rail transit owner/operators (SD 1580/82-2022-01).[96] Prior to the issuance of SD 1580/82-2022-01, the TSA Administrator instructed TSA to include Defense Connector Railroads to the applicability pool for SD 1580/82-2022-01 and SD 1580-21-01. This was done in consultation with the Department of Defense and Federal Railroad Administration officials. The justification for this expanded applicability was and is the threat posed to the rail network by hostile nation state actors.

1.7.3 PTPR

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. While PTPR typically includes buses, for purposes of this proposed rulemaking, PTPR is limited to rail transit and passenger rail. The sole long-distance inter-city passenger railroad in the contiguous United States is Amtrak, which has a pre-pandemic annual ridership of approximately 31.7 million.[97] Amtrak 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.[98] Nearly half of all Amtrak trains operate at top speeds of 100

---

[95] *See* Surface Transportation IC-2021-01: Enhancing Surface Transportation Cybersecurity at https://www.tsa.gov/sites/default/files/20211201_surface-ic-2021-01.pdf. Accessed on Oct. 19, 2022.
[96] *See* SD 1580/82-2022-01: Rail Cybersecurity Mitigation Actions and Testing at https://www.tsa.gov/sites/default/files/sd-1580-82-2022-01.pdf. Accessed on Oct. 19, 2022.
[97] American Public Transportation Association (APTA). Apr. 2019. 2019 Public Transportation Fact Book. https://www.apta.com/wp-content/uploads/APTA_Fact-Book-2019_FINAL.pdf. Accessed on June 15, 2023.
[98] *Id.* at 30

mph or greater. In fiscal year 2021, Amtrak customers took nearly 12.2 million trips.[99]

Freight railroads provide the tracks for most passenger rail operations. For example, seventy-two 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.[100]

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 by Amtrak. It runs from Boston through New York City, Philadelphia, Baltimore, and terminus in Washington, D.C.

Amtrak and other passenger railroads also host freight rail operations. In fact, the Northeast Corridor is the busiest rail line in North America, with approximately 2,200 Amtrak, commuter and freight trains operating over some portion of the Washington-Boston route each day.[101] As with freight railroads, passenger railroads are subject to safety regulations put forth and enforced

---

[99] National Railroad Passenger Corporation d/b/a Amtrak. Apr. 2022. Amtrak FY 2021 Company Profile: For the Period October 1, 2020 – September 30, 2021. https://www.amtrak.com/content/dam/projects/dotcom/english/public/documents/corporate/nationalfactsheets/Amtrak-Company-Profile-FY2021-030922.pdf. Accessed on June 4, 2023.

[100] *Id.* at 3

[101] *Id.* at 4

by the FRA.[102] TSA administers and enforces passenger rail security regulations contained in 49 CFR part 1582.

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 nearly 6 billion unlinked passenger trips in 2020 across the various public transportation modes.[103] Note that this represents a significant decline, due to changes in behavior due to the Covid-19 pandemic. Nonetheless, reliable public transit is an integral part of society and data will be monitored in future years to see if ridership patterns revert towards the mean. Nationwide, 3.8 million Americans commute to work on transit, equivalent to approximately 2.5 percent of workers. In major metropolitan areas, like New York City, nearly 28 percent of commuters rely on public transportation for their daily commute.[104] Rail transit is a critical part of the overall public transit system, representing about 52 percent of all passenger miles traveled on public transit.[105]

As discussed previously, TSA assesses all the proposed rule requirements as new and presents a baseline level of compliance of zero. However, TSA recognizes owner/operators may have

---

[102] An example of an action unrelated to this proposal but serves here to indicate the importance and priority of cybersecurity for safety is the recent FRA regulation. *See* Federal Railroad Administration. March 2022. Railroad Workplace Safety, 49 CR 214. https://www.federalregister.gov/documents/2022/03/17/2022-05625/railroad-workplace-safety. Accessed on August 31, 2023.

[103] American Public Transportation Association. Jan. 2023. 2022 Public Transportation Fact Book. https://www.apta.com/research-technical-resources/transit-statistics/public-transportation-fact-book. Accessed on June 15, 2023. 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.

[104] *Id.* at 12

[105] 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.

started implementing a cybersecurity risk management program previously. In December 2021, TSA issued SDs to passenger rail and rail transit owner/operators (the SD 1582-21-01 series): (1) designation of a cybersecurity coordinator and alternate; (2) reporting of cybersecurity incidents to CISA within 24 hours; (3) developing and implementing a CIRP to reduce the risk of an operational disruption; and (4) completing a cybersecurity vulnerability assessment to identify potential gaps or vulnerabilities in their systems. 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 measures.[106] On October 18, 2022, TSA issued a SD imposing performance-based cybersecurity requirements on higher-risk freight railroads, passenger rail, and rail transit owner/operators (SD 1580/82-2022-01).[107]

1.7.4 Highway and Motor Carrier

49 CFR Part 1584 is overall Highway and Motor Carrier but for this proposed CRM rulemaking, the provisions are applicable only to over-the-road-bus (OTRB). According to the 2020 Motorcoach Census, there are 1,717 companies that operated 27,753 motorcoaches in the United States and that across the U.S. and Canada, nearly 125 million passenger trips were provided in 2020.[108] While commuter services is not the largest type of service offered by the carriers, the services provided by the OTRB providers are a necessary and important part of transportation for Americans. 71 OTRB owner/operators fall within the applicability of the rule as they provide fixed-route service that originates, travels through, or ends in a geographic location identified in

---

[106] *See* Information Circular: Surface Transportation IC-2021-01: Enhancing Surface Transportation Cybersecurity at https://www.tsa.gov/sites/default/files/20211201_surface-ic-2021-01.pdf. Accessed on Oct. 19, 2022.
[107] *See* SD 1580/82-2022-01: Rail Cybersecurity Mitigation Action and Testing at https://www.tsa.gov/sites/default/files/sd-1580-82-2022-01.pdf. Accessed on Oct. 19, 2022.
[108] American Bus Association (ABA). Jan. 7, 2022. Motorcoach Census: A Study of the Size and Activity of the Motorcoach Industry in the United States and Canada in 2020. https://www.buses.org/wp-content/uploads/2024/02/Motorcoach_Census_Survey_2020.pdf. Accessed on June 9, 2023.

49 CFR 1584 Appendix A.[109] Currently, it is recommended via information circular (IC) that cybersecurity incidents are reported to CISA; this rulemaking will codify and make mandatory that reporting requirement via methods prescribed from TSA. TSA anticipates reports would be communicated, as needed, from CISA.

1.7.5 Pipeline

The national pipeline system consists of more than 2.96 million miles of networked pipelines transporting hazardous liquids, natural gas, and other liquids and gases for energy needs and manufacturing.[110] Although most pipeline infrastructure is buried underground, operational elements such as compressors, metering, regulating, pumping stations, aerial crossings, and storage tanks are typically located above ground. Under operating pressure, the pipeline system is used as a conveyance to deliver resources from source location to destination. They are monitored and moderated through automated ICS, such as SCADA systems. These systems use remote sensors, signals, and preprogramed parameters to activate valves and pumps to maintain flows within tolerances. Pipeline systems supply energy commodities and raw materials across the country to utility entities, airports, military sites, and to the Nation's industrial and manufacturing sectors. Vital components of the mode include assets, components, and industrial automated, semi-automated, and manual control systems.

As discussed previously, TSA assesses all the proposed rule requirements as new and presents a baseline level of compliance of zero. However, TSA recognizes that owner/operators may have

---

[109] Appendix A is available via the Code of Federal Regulations at https://www.ecfr.gov/current/title-49/subtitle-B/chapter-XII/subchapter-D/part-1584/appendix-Appendix%20A%20to%20Part%201584. Accessed on June 15, 2023.

[110] Mileage is available via the Pipeline and Hazardous Materials Safety Administration at https://www.phmsa.dot.gov/data-and-statistics/pipeline/annual-report-mileage-summary-statistics. Accessed on November 30, 2023.

started implementing a cybersecurity risk management program previously, including in response to TSA security directives issued on July 21, 2021 and July 26, 2021. The first directive required certain pipeline owner/operators to: (1) designate a primary and alternate cybersecurity coordinator; (2) report cybersecurity incidents to CISA within 24 hours of identification of a cybersecurity incident;[111] and (3) review TSA's pipeline guidelines,[112] assess their current cybersecurity posture, and identify remediation measures to address the vulnerabilities and cybersecurity gaps.[113] The second directive 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. It also required owner/operators to develop and adopt a CIRP to reduce the risk of operational disruption should their IT and/or OT systems be affected by a cybersecurity incident.[114]

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 this, 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

---

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

[112] *See* Section I.F. of preamble for more information on TSA's guidelines for the pipeline owner/operators.

[113] 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.

[114] *See* SD Pipeline-2021-01B: Enhancing Pipeline Cybersecurity at https://www.tsa.gov/sites/default/files/sd_pipeline-2021-01b_05-29-2022.pdf for a version of the SD with the prescriptive requirements initially imposed. Accessed on Oct. 19, 2022.

imposing performance-based, rather than prescriptive, security measures.[115] The current directive in the 2021-02 series is 2021-02D, effective July 27, 2023. This directive requires certain pipeline operators to do the following:

- Establish and implement a TSA-approved Cybersecurity Implementation Plan that describes the specific cybersecurity measures employed 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 significant impacts on necessary capacity, as defined in the SD, should the IT and/or OT systems of a gas or liquid pipeline and rail be affected by a cybersecurity incident.
- Establish a Cybersecurity Assessment Plan and submit it to TSA for approval. The plan describes how the owner/operator will proactively and regularly assess the effectiveness of cybersecurity measures and identify and resolve device, network, and/or system vulnerabilities. The plan also requires covered operators to submit an annual report to TSA of the result of the assessments conducted.

[115] In order to support owner/operators, TSA has developed multiple resources to assist with SD compliance and would continue to provide resources for this proposed rule. Such resources include responses to frequently asked questions, an information supplement that crosswalks the SD requirements with NIST. TSA has also provided examples of CIPs and CAPs to owner/operators and would continue to provide these resources.

2 POPULATIONS AFFECTED, QUANTITIES, UNIT COSTS, AND OTHER ASSUMPTIONS

In this section, TSA presents the population of entities affected, data and assumptions on current practices, and expected changes resulting from the implementation of the proposed rule. TSA uses this information to complete its RIA and measure the costs from the proposed rule over a ten-year period of analysis, discounted at 3 and 7 percent, beginning in 2024. The cost estimates are presented in 2022 dollars.

This information — and the assumptions made as a result — includes populations affected by the proposed rule, compensation rates, and burden estimates for entities to complete the requirements of the proposed rule. This section also presents estimates and assumptions made about other cost factors associated with the proposed rule including training costs, equipment costs, and recordkeeping.

2.1 Affected Transportation Populations

This section provides information on the criteria for inclusion or applicability of the proposed rule as applied to each affected transportation mode and details the associated owner/operators used to inform cost impacts. As discussed in the preamble, TSA applies a risk-based approach for determining applicability. Requirements are focused on higher-risk operations based on considerations such as dependency on commuting options, passenger safety, and supply chain impacts that could affect national security, including economic security. TSA has made the requirements in the SDs, and additional cybersecurity resources, available to all surface transportation owner/operators, including those not covered by the SDs and not within the proposed scope of applicability, encouraging their voluntary adoption. But this action is

voluntary; not required by TSA.

2.1.1 Freight Rail Population

Section 1580 details the criteria for inclusion or applicability of the proposed rule for freight railroads. The criteria specifically include the following:

- Is a Class I railroad as defined in current 49 CFR 1580.3;[116] or
- Is a Class II or III railroad that:
  - Transports one or more of the categories and quantities of Rail Security-Sensitive Materials[117] in a High Threat Urban Area;[118]
  - 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 years before the effective date of the final rule or in any calendar year after the effective date;[119]
  - Is designated as a Defense Connector Railroad by DoD; or

[116] 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.

[117] 49 CFR 1580.3.

[118] Appendix A to 49 CFR part 1580.

[119] TSA reviewed historical statistics from the FRA to discern a threshold of annual train miles. The 400,000 train-miles threshold provided a clear break-point 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).

- 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.[120]

These criteria use a risk-based approach that covers approximately 73 freight railroads of the 620 freight railroads operating in the United States. The six Class I account for approximately 68 percent of freight rail mileage, 88 percent of employees, and 94 percent of revenue.[121] In addition, TSA estimates 25 of the 73 freight railroads represent small entities as shown in Section 6.5.1.[122] The proposed applicability for CRM program requirements expands the applicability of the SDs to include an additional nine railroads, all of which operate in excess of an average 400,000 train miles per year. This expansion covers additional railroads where the effects of a service issue or interruption could cause significant disruption to the overall industry's service capacity. TSA consulted FRA for train-mile data in order to identify freight rail carriers whose volume placed them in the upper echelon of freight carriers on the Nation's rail network. FRA provided 10 years' worth of train mile data. After studying this data, TSA identified a natural breaking point at 400,000 average train miles (over a three-year period) which identified nine railroads which were not covered by the SD, but were major connecting railroads on the rail network.

2.1.2 PTPR Population

Section 1582 details the criteria for inclusion or applicability of the proposed rule for PTPR. The

---

[120] 49 CFR 1582.101.

[121] Association of American Railroads (AAR). Jul. 2023. Freight Rail Facts & Figures: Capacity and Service. https://www.aar.org/facts-figures#4-capacity-amp-service. Accessed on July 30, 2023.

[122] TSA uses Small Business Administration (SBA) size standards to make small entity determinations. SBA standards are available at https://www.sba.gov/document/support-table-size-standards. Accessed on July 28, 2023. TSA calculates that 34.25 percent of the freight rail owner/operators are considered small under the SBA size standards (25 ÷ 73 = 34.25%). The remaining 65.75% are considered not small.

criteria, which is based on ridership, specifically include the following:

- Is Amtrak (also known as the National Railroad Passenger Corporation) or other 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 railroads 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."

These proposed criteria 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.[123] According to American Public Transportation Association volume data, 34 rail transit and passenger railroads of the approximately 92 rail transit and passenger railroads operating in the

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

United States would meet these risk-based criteria.[124] In addition, TSA estimates none of the 34 PTPR systems represent small entities.[125] The proposed applicability for this rulemaking does not include three systems that currently fall under the security training requirements in Part 1582 because these systems did not meet the ridership threshold proposed for this rulemaking based on the specific risks the rule is intended to address.

2.1.3 OTRB Population

Section 1584.107 details the criteria for inclusion or applicability of the proposed rule for over-the-road-buses (OTRBs). 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 currently subject to TSA's regulatory requirements to report security incidents,[126] be required to report both physical security and cybersecurity incidents. TSA estimates that 71 OTRB owner/operators would be subject to this requirement.

According to TSA internal data, these 71 owner/operators are currently subject to TSA's regulatory requirements to report security incidents. These owner/operators would also be required to report cybersecurity incidents under the proposed rule. TSA estimates the majority of the covered owner/operators represent small entities.[127] The scope of regulation for these

---

[124] American Public Transportation Association (APTA). Jan. 2023. 2022 Public Transportation Fact Book. https://www.apta.com/research-technical-resources/transit-statistics/public-transportation-fact-book/. Accessed June 27, 2023. For purposes of this analysis, PTPR is comprised of 92 Transit Rail and Passenger Railroad systems made up of 30 Commuter Rail, 15 Heavy Rail, 23 Light Rail, and 24 Streetcar.

[125] TSA uses Small Business Administration (SBA) size standards to make small entity determinations. SBA standards are available at https://www.sba.gov/document/support-table-size-standards. 33 of the 34 Rail Transit and Passenger Rail entities covered by the proposed rule are owned or operated by government jurisdictions with populations greater than 50,000. The entity that is owned or operated as a private company has annual revenue exceeding the SBA Size Standard for NAICS 485112 (Commuter Rail Systems) of $41.5 million.

[126] 49 CFR 1570.203.

[127] TSA uses Small Business Administration (SBA) size standards to make small entity determinations. SBA standards are available at https://www.sba.gov/document/support-table-size-standards.

owner/operators is narrower than other modes as the risk environment and technology interaction is different for this population. Note that for several of the provisions, including applicability and familiarization, TSA utilizes occupations and wage rates consistent with the other modes. This determination was made to maintain consistency across each mode and is not intended to result in additional requirements. The assumption is these provisions will be undertaken by an individual with the equivalent responsibility of the stated occupation as the CRM requirements applicable to other modes, but not OTRB who do not fall under the same requirements or require the express designation of specific titles. While TSA has decided not to impose the full scope of the proposed CRM program requirements at this time, it may revisit this decision in the future.

2.1.4 Pipelines Population

Section 1586 details the criteria for inclusion or applicability of the proposed rule for pipelines. The criteria are distinct from existing standards and were developed for this proposed CRM rule. The intent of the specific criteria is to ensure that control rooms that operate pipeline systems that cumulatively meet certain thresholds are covered under the CRM. A cybersecurity incident resulting in an operational disruption of a control room that operates multiple pipeline systems that cumulatively meet the threshold could have a significant impact on pipeline delivery. For owner/operators of hazardous liquid pipelines, the criteria specifically include the following:

- The hazardous liquid pipelines are subject to 49 CFR part 195 and—
    - Annually deliver 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

- Are 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.[128]

- Operate a primary control room that is responsible for multiple systems 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.[129]

For owner/operators of natural gas and other gas pipelines, the criteria and thresholds were developed by TSA specifically for this proposed rule. The criteria are similar to that used by TSA to identify critical pipeline operators, based on risk, as set forth in the statutory requirement to identify the 100 most critical pipeline operators.[130] The proposed CRM program requirements includes each company that:

- Owns or operates a natural or other gas system subject to 49 CFR part 192 and—
  - 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

[128] *See* proposed 49 CFR part 1586 for a definition of High Consequence Area and a discussion of Terms in subsection D of this section.
[129] The criteria for 70,000 barrels is pending coordination with the Defense Logistics Agency. This amount conforms to what TSA uses to identify critical pipeline systems ("Top 100").
[130] *See* 6 U.S.C. 1207(b).

effective date of the final rule, or any single calendar year after the effective date of the final rule;

- 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 in excess of 200 segment miles that could affect a High Consequence Area.

- Owns or operates a primary control room responsible for multiple natural gas or other pipeline systems regulated under 49 CFR part 192 and the combined total annual delivery for those 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 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.

For owners/operators of Liquefied Natural Gas (LNG) facilities, the proposed CRM program apply to facilities that import natural gas or operate as peak shaving facilities.[131]

TSA estimates this applicability would affect 115 pipelines, of which 66 are natural gas, 39 are

[131] 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.

hazardous liquids, 9 are LNG, and 1 is chemical. The systems and facilities impacted account for approximately 91 percent of the total annual volume transported in the United States. TSA estimates 23 of the 115 pipeline systems and facilities represent small entities.[132]

2.2 Growth and Turnover

TSA calculates entity growth rates using a compound average growth rate for each mode except pipeline, which due to the nature of the industry, is assumed to not experience growth and will remain flat or static. Similarly, TSA also assumes Class I freight railroads will remain static.[133] Based on AAR data, TSA estimates a freight rail entity growth rate of 0.85 percent per year for Class II and III freight railroads.[134] TSA uses the Department of Transportation's National Transit Database (NTD) to estimate a PTPR's entity growth rate of 2.19 percent per year.[135] Finally, TSA uses U.S. Census Bureau Economic Census information to estimate a OTRB entity growth rate of 2.50 percent per year.[136] While there is a process available for affected

---

[132] TSA uses Small Business Administration (SBA) size standards to make small entity determinations. SBA standards are available at https://www.sba.gov/document/support-table-size-standards.

[133] As a result, TSA does not apply freight rail growth to the six Class I freight rail entities.

[134] TSA derives the compound annual growth rate (CAGR) for Class II and III freight railroads based on 2017 and 2007 data obtained from the AAR Railroad Facts (2020 edition)
and AAR U.S. Freight Railroad Statistics (2010 edition). 0.85 percent = (613 ÷ 563)^(1 ÷ (2017-2007))-1. p. 4. Accessed from, respectively: https://www.aar.org/facts-figures ; https://rosap.ntl.bts.gov/view/dot/5861. Accessed July 29, 2021.

[135] TSA calculates the PTPR entity growth rate as the compound average growth in entities reported by the Department of Transportation's National Transit Database (NTD), Agencies by Mode dataset. The NTD data show that there were 62 passenger transit rail entities in 2011 and 77 in 2021. TSA calculates the compound annual growth rate between 2011 and 2021 as 2.19% ((77 ÷ 62)^(1 ÷ 10) – 1). U.S. Department of Transportation. 2021. "2021 Annual Database Agency Mode service." https://www.transit.dot.gov/ntd/data-product/2021-annual-database-agency-mode-service. Accessed July 29, 2021.

[136] Growth rate is equal to CAGR from 2007 to 2017 of the sum of establishment populations of the following NAICS codes: 4859 (other transit and ground passenger transportation system), 4855 (charter bus industry), 485113 (bus and other motor vehicle transit systems), and 4852 (interurban and rural bus transportation). These NAICS codes were chosen because they were seen as representative of the general bus industry. CAGR = [(7,704 ÷ 6,019)^(1÷ (2017 - 2007))] – 1 = 0.0250. U.S. Census Bureau, 2007 Economic Census, EC1700BASICAll Sectors: Summary Statistics for the U.S., States, and Selected Geographies: 2017 https://data.census.gov/table?q=EC1700BASICAll+Sectors&tid=ECNBASIC2017.EC1700BASIC. Accessed on September 19, 2023. U.S. Census Bureau, 2007 County Business Patterns and 2007 Economic Census. 2007 SUSB Annual Data Tables by Establishment Industry. https://www.census.gov/data/tables/2007/econ/susb/2007-susb-annual.html. Accessed on September 19, 2023.

owner/operators to be removed from the scope of the rule, via TSA approving documentation provided by the operator that they no longer meet the criteria, TSA assumes this will be rare. For purposes of the calculations, TSA assumes there is not entity turnover such that once an entity is subject to the applicability of the rule, they would always be in scope and do not drop out.[137]

To calculate employee growth rates, TSA takes 2031 projected employment figures from the U.S. Bureau of Labor Statistics (BLS) National Employment Matrix per mode and divides by 2021 employment figures then equally apportions the resulting growth over ten-years.

Using this approach, TSA estimates a freight rail employee growth rate of 0.42 percent per year.[138] Similarly, PTPR's employee growth rate is 1.11 percent.[139] However, as OTRB applicability in the proposed rule relates to reportable incidents, employment levels are not included in the population and cost analysis. Finally, TSA estimates pipelines employee growth rate as 0.62 percent per year.[140]

---

[137] Section 1570.105(c) provides details on how an entity may be exempted from being a covered owner/operator under the rule due to permanent changes in operations to the extent that the applicability criteria in parts 1580, 1582, 1584, or 1586 no longer apply. TSA recognizes that an entity can technically no longer be subject to the rule due to changes in applicability, but TSA believes this unlikely and thus assumes no entity turnover.

[138] TSA calculates the freight employee projected growth rate as the compound average growth in employment for all occupations in NAICS 482000 Rail Transportation, based on BLS Employment Matrix Data. BLS data show 2021 employment as 146,200 and 2031 employment as 152,400. The growth rate is calculated as (152,400 ÷ 146,200)^(1 ÷ 10) -1 = 0.42%. U.S. Bureau of Labor Statistics, National Employment Matrix, Employment by industry, occupation, and percent distribution, 2021 and projected 2031. https://www.bls.gov/emp/. Accessed July 13, 2023.

[139] TSA calculates the PTPR employee projected growth rate as the compound average growth in employment for all occupations in NAICS 485000 Transit and Ground Passenger Transportation, based on BLS Employment Matrix Data. BLS data show 2021 employment as 374,600 and 2031 employment as 418,500. The growth rate is calculated as (418,500 ÷ 374,600)^(1 ÷ 10) - 1 = 1.11%. U.S. Bureau of Labor Statistics, National Employment Matrix, Employment by industry, occupation, and percent distribution, 2021 and projected 2031. https://www.bls.gov/emp/. Accessed July 13, 2023.

[140] U.S. Bureau of Labor Statistics, National Employment Matrix, Employment by industry, occupation, and percent distribution, 2021 and projected 2031. https://www.bls.gov/emp/. Accessed July 13, 2023. TSA calculates the Pipeline employee projected growth rate as the compound average growth in employment for all occupations within the applicable pipeline NAICS. For purposes of this analysis, TSA is summing the employment in NAICS 486100 Pipeline Transportation of Crude Oil, 486900 Other Pipeline Transportation, and 486200 Pipeline Transportation of Natural Gas, based on BLS Employment Matrix Data. BLS data show 2021 employment as 49,900 and 2031 employment as 53,100. The growth rate is calculated as (53,100 ÷ 49,900)^(1 ÷ 10) - 1 = 0.62%.

TSA estimates employee turnover specific to each mode. For freight rail, TSA estimates employee turnover at 4 percent, consistent with data from the U.S. Railroad Retirement Board.[141] For PTPR, TSA estimates employee turnover is 12.96 percent, consistent with industry employment projections from the BLS.[142] For Pipeline, TSA estimates employee turnover is 13.67 percent, consistent with industry employment projections from the BLS.[143] TSA does not estimate employee turnover for OTRB due to no requirements in the proposed rule affecting the OTRB general employee population.

Table 2-1 presents a breakdown of model entity populations over the 10 year period of analysis.[144] Table 2-2 presents a breakdown of model employee populations, employee growth,

---

[141] U.S. Railroad Retirement Board. Twenty-Seventh Actuarial Valuation of the Assets and Liabilities under the Railroad Retirement Acts as of December 31, 2016 with Technical Supplement. P 82. Table S-36: Withdrawal experience of railroad employees during calendar years 2011–2014, by attained age and years of service. The table presents a crude rate per 100 of the actual net withdrawals. (https://rrb.gov/sites/default/files/2018-09/valuation.pdf). TSA uses the "All ages crude rate per 100" for all years of service from the 25-34 and 35-44 age ranges. The growth rate is calculated as ((5.1 + 3.1) / 2) = 4.1 or approximately 4 percent. This is the number of people leaving and not re-entering (Withdrawals less re-entrants rate). Accessed July 29, 2021.

[142] U.S. Bureau of Labor Statistics, Employment Projections Program "Table 1.10 Occupational Separations and Opening, Projected 2021-31." https://www.bls.gov/emp/tables/occupational-separations-and-openings.htm. Accessed on April 21, 2023. To calculate PTPR turnover rate, TSA based its estimate on the following Employment Matrix titles (codes): Transit and railroad police (33-3052), Subway and streetcar operators (53-4041), and Bus drivers, transit and intercity (53-3052). TSA calculated the PTPR turnover rate from labor force exist from these three employment titles to be 7.58 percent in 2021. 7.58% = (3,500 transit and railroad police × 3.0% labor force exists + 10,600 subway and streetcar operators × 4.2% labor force exists + 159,900 bus drivers, transit and intercity × 7.9% labor force exists) ÷ (3,500 transit and railroad police + 10,600 subway and streetcar operators + 159,900 bus drivers, transit and intercity). TSA then calculated the PTPR turnover rate from occupational transfers from these three employment titles to be 5.38 percent in 2021. 5.38% = (3,500 transit and railroad police × 5.1% occupational transfers + 10,600 subway and streetcar operators × 6.7% occupational transfers + 159,900 bus drivers, transit and intercity × 5.3% occupational transfers) ÷ (3,500 transit and railroad police + 10,600 subway and streetcar operators + 159,900 bus drivers, transit and intercity). Finally, TSA sums the labor force exit rate (7.58%) with the occupational transfer rate (5.38%) to calculate a total PTPR turnover rate of 12.96 percent.

[143] U.S. Bureau of Labor Statistics, Employment Projections Program "Table 1.10 Occupational Separations and Opening, Projected 2021-31." https://www.bls.gov/emp/tables/occupational-separations-and-openings.htm. Accessed on April 21, 2023. TSA added the number of new employees replacing quits to the number of occupational transfers for the 53-0000 series set of occupations, "Transportation and moving" and weighted by the employment of the industry.

[144] TSA assumes Class I freight railroads will remain static. Therefore, TSA does not include growth to the six Class I freight rail entities but adds them in after applying growth to the class II and III impacted population as show in column a of Table 2-1.

and employee turnover based on the respective rates discussed above.

Table 2-1: Population Growth and Turnover for Modal Entities

Year	Freight Rail			PTPR			OTRB			Pipelines	
	Covered Entities	New Entities	Entity Growth	Covered Entities	New Entities	Entity Growth	Covered Entities	New Entities	Entity Growth	Covered Entities	New Entities
	$a = 67 \times (1 + 0.85\%) \wedge (Y_n - 1) + 6$	$b = 67 \times (1 + 0.85\%) \wedge (Y_n - 1) + 6 - \sum b_{y1}..b_{yn-1}$	$c = a_{yn} - a_{yn-1}$	$d = 34 \times (1 + 2.19\%) \wedge (Y_n - 1)$	$e = 34 \times (1 + 2.19\%) \wedge (Y_n - 1) - \sum d_{y1}..d_{yn-1}$	$f = d_{yn} - d_{yn-1}$	$g = 71 \times (1 + 2.50\%) \wedge (Y_n - 1)$	$h = 71 \times (1 + 2.50\%) \wedge (Y_n - 1) - \sum g_{y1}..g_{yn-1}$	$i = g_{yn} - g_{yn-1}$	$j = 115$	$k_{y1} = 115$ $k_{yn} = 0$
1	73.00	73.00	0.00	34.00	34.00	0.00	71.00	71.00	0.00	115.00	115.00
2	73.57	0.57	0.57	34.74	0.74	0.74	72.78	1.78	1.78	115.00	0.00
3	74.14	0.57	0.57	35.51	0.77	0.77	74.59	1.81	1.81	115.00	0.00
4	74.72	0.58	0.58	36.28	0.77	0.77	76.46	1.87	1.87	115.00	0.00
5	75.31	0.59	0.59	37.08	0.80	0.80	78.37	1.91	1.91	115.00	0.00
6	75.90	0.59	0.59	37.89	0.81	0.81	80.33	1.96	1.96	115.00	0.00
7	76.49	0.59	0.59	38.72	0.83	0.83	82.34	2.01	2.01	115.00	0.00
8	77.09	0.60	0.60	39.57	0.85	0.85	84.40	2.06	2.06	115.00	0.00
9	77.69	0.60	0.60	40.43	0.86	0.86	86.51	2.11	2.11	115.00	0.00
10	78.30	0.61	0.61	41.32	0.89	0.89	88.67	2.16	2.16	115.00	0.00

Note: Values rounded to hundredth decimal place unless otherwise displayed.

Table 2-2: Population Growth and Turnover for Modal Employees

Year	Freight Rail			PTPR			Pipelines		
	Covered Employees	Employee Growth	Employee Turnover	Covered Employees	Employee Growth	Employee Turnover	Covered Employees	Employee Growth	Employee Turnover
	$a = 116{,}960 \times (1 + 0.42\%) \wedge (Y_n - 1)$	$b = a_{yn} - a_{yn-1}$	$c = a \times 4.00\%$	$d = 299{,}680 \times (1 + 1.11\%) \wedge (Y_n - 1)$	$e = d_{yn} - d_{yn-1}$	$f = d \times 12.96\%$	$g = 39{,}920 \times (1 + 0.62\%) \wedge (Y_n - 1)$	$h = g_{yn} - g_{yn-1}$	$l = g \times 13.67\%$
1	116,960.00	0.00	0.00	299,680.00	0.00	0.00	39,920.00	0.00	0.00
2	117,451.23	491.23	4,698.05	303,006.45	3,326.45	39,269.64	40,167.50	247.50	5,490.90
3	117,944.53	493.30	4,717.78	306,369.82	3,363.37	39,705.53	40,416.54	249.04	5,524.94
4	118,439.89	495.36	4,737.60	309,770.52	3,400.70	40,146.26	40,667.13	250.59	5,559.20
5	118,937.34	497.45	4,757.49	313,208.98	3,438.46	40,591.88	40,919.26	252.13	5,593.66
6	119,436.88	499.54	4,777.48	316,685.60	3,476.62	41,042.45	41,172.96	253.70	5,628.34
7	119,938.51	501.63	4,797.54	320,200.81	3,515.21	41,498.02	41,428.23	255.27	5,663.24
8	120,442.26	503.75	4,817.69	323,755.04	3,554.23	41,958.65	41,685.09	256.86	5,698.35
9	120,948.11	505.85	4,837.92	327,348.72	3,593.68	42,424.39	41,943.54	258.45	5,733.68
10	121,456.09	507.98	4,858.24	330,982.29	3,633.57	42,895.30	42,203.59	260.05	5,769.23

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed. Formulas with X_{yn-1} in year one are equal to the initial value of X_{y1}.

2.3 Compensation

To satisfy the requirements of the rule, various owner/operator staff would perform a number of different functions. To account for the cost associated with such tasks, TSA identifies job titles that would likely be associated with the various provisions of this proposed rulemaking, or something equivalent, and associated BLS standard occupational codes. For instance, under the proposed rule, the accountable executive is an individual with the authority and responsibility of a C-Suite level executive for which TSA identifies the chief executive occupational code as being representative of this function. For purposes of this RIA, the accountable executive is not assumed to be the chief executive but that occupational code is the most comparable in terms of requirements that the accountable executive would undertake as part of carrying out the provisions of the proposed rule.

Job titles include: a manager and accountable executive, cybersecurity coordinator, cybersecurity operations manager (COM), cybersecurity analyst, network and computer systems administrator, audit manager, administrative assistant, and attorney. For pipeline owner/operators, there would also be a physical security coordinator. Additionally, TSA calculates an average wage for those provisions that impact all occupations, as well as all cybersecurity positions.

TSA identifies representative occupational codes for each of the job titles and utilizing BLS Occupational Employment and Wage Statistics (OEWS) survey, identified an average wage for each.[145] Table 2-3 presents a crosswalk of the job titles identified to the corresponding OEWS

[145] Bureau of Labor Statistics. May 2022 Occupational Employment and Wage Statistics. https://www.bls.gov/oes/2022/may/oessrci.htm. Accessed on May 1, 2023. TSA notes that 2023 publication is based on 2022 data.

Occupational Code.

Table 2-3: Job Titles and Occupation Codes

Job Titles	Occupation Code
Cybersecurity Coordinator	11-3021 Computer and Information Systems Managers
Cybersecurity Operations Manager	11-3021 Computer and Information Systems Managers
Cybersecurity Analyst	15-1212 Information Security Analyst
Network and Computer Systems Administrator	15-1244 Network and Computer Systems Administrator
All Liquid Pipeline Cyber Positions	15-0000 Computer and Mathematical Occupations
Audit Manager	11-3012 Administrative Services Managers
All Liquid Pipeline Employees	00-0000 All Occupations
Administrative Assistant	43-6010 Secretaries and Administrative Assistants
Attorney	23-1011 Lawyers
Accountable Executive	11-1011 Chief Executive

To estimate the cost for each job title, TSA uses the average or mean salary for each occupational code identified above from the BLS OEWS. To account for non-salary compensation, such as health and retirement benefits, TSA calculates a load factor based on information from the BLS Employer Costs for Employee Compensation (ECEC) survey. Specifically, TSA divides the total civilian average compensation ($33.17) by the average wage and salaries for the production, transportation, and material moving occupational group ($22.34) which results in a load factor of 1.48.[146] Applying this load factor to occupational wages provides a fully-loaded compensation rate for each occupation.[147] Identified wages are held constant throughout the period of analysis.

2.3.1 Freight Compensation

For freight rail, TSA uses the North American Industry Classification System (NAICS) code of

[146] Bureau of Labor Statistics. Dec. 2022. Employer Costs for Employee Compensation, Table 2. Employer costs per hour worked for employee compensation and costs as a percent of total compensation. Civilian workers, production, transportation, and material moving occupational group (Total compensation of $33.17 divided by wages and salaries of $22.34 yields the applicable load factor of 1.48 to represent the non-salary cost adjustment). Values includes workers in the private nonfarm economy, except those in private households, and workers in the public sector, except the Federal government. Accessed on April 4, 2023. https://www.bls.gov/news.release/archives/ecec_03172023.htm

[147] Fully-loaded compensation rate (loaded wage) = [unloaded wage] × 1.48.

482000 - Rail Transportation as the universe from which to pull the occupation-specific base wage.[148] Table 2-4 presents the estimated unloaded and loaded wage rates for each job title identified.

Table 2-4: Associated Labor Rates for Employees in the Freight Rail Industry

Job Title	NAICS 482000 Occupation Title	Unloaded Wage	Loaded Wage
		a	b = a × 1.48
Cybersecurity Coordinator	11-3021 Computer and Information Systems Managers	$85.88	$127.10
Cybersecurity Operations Manager	11-3021 Computer and Information Systems Managers	$85.88	$127.10
Cybersecurity Analyst	15-1240 Database and Network Administrators and Architects	$45.50	$67.34
Network and Computer Systems Administrator	15-1244 Network and Computer Systems Administrator	$43.67	$64.63
All Freight Rail Cyber Positions	15-0000 Computer and Mathematical Occupations	$65.73	$97.28
Audit Manager	11-3012 Administrative Services Managers	$62.60	$92.65
All Freight Rail Employees	00-0000 All Occupations	$35.94	$53.19
Administrative Assistant	43-6010 Secretaries and Administrative Assistants	$27.31	$40.42
Attorney	23-1011 Lawyers	$87.98	$130.21
Accountable Executive	11-1011 Chief Executive	$136.89	$202.60

Note: Values rounded to hundredth decimal place unless otherwise displayed.

2.3.2 PTPR Compensation

For PTPR, TSA uses NAICS 485000 – Transit and Ground Passenger Transportation as the universe from which to pull the occupation-specific base wage.[149] The result for each job title is shown in Table 2-5.

[148] BLS. May 2022 National Industry-Specific Occupational Employment and Wage Estimates. NAICS 482000 - Rail Transportation. Accessed May 1, 2023. https://www.bls.gov/oes/2022/may/naics3_482000.htm

[149] BLS. May 2022 National Industry-Specific Occupational Employment and Wage Estimates. NAICS 485000 – Transit and Ground Passenger Transportation. Accessed May 1, 2023. https://www.bls.gov/oes/2022/may/naics3_485000.htm

Table 2-5: Associated Labor Rates for Employees in the PTPR Industry

Job Title	Occupation Title	Unloaded Wage	Loaded Wage
		a	b = a × 1.48
Cybersecurity Coordinator	11-3021 Computer and Information Systems Managers	$71.50	$105.82
Cybersecurity Operations Manager	11-3021 Computer and Information Systems Managers	$71.50	$105.82
Cybersecurity Analyst	15-1240 Database and Network Administrators and Architects	$42.67	$63.15
Network and Computer Systems Administrator	15-1244 Network and Computer Systems Administrator	$42.99	$63.63
All PTPR Cyber Positions	15-0000 Computer and Mathematical Occupations	$48.15	$71.26
Audit Manager	11-3012 Administrative Services Managers	$40.84	$60.44
All PTPR Employees	00-0000 All Occupations	$21.10	$31.23
Administrative Assistant	43-6010 Secretaries and Administrative Assistants	$20.32	$30.07
Attorney	23-1011 Lawyers	$49.11	$72.68
Accountable Executive	11-1011 Chief Executive	$90.75	$134.31

Note: Values rounded to hundredth decimal place unless otherwise displayed.

2.3.3 OTRB Compensation

For OTRB, TSA uses NAICS 485000 – Transit and Ground Passenger Transportation as the universe from which to pull the occupation-specific base wage.[150] The result for each job title is shown in Table 2-6.

Table 2-6: Associated Labor Rates for Employees in the OTRB Industry

Job Title	Occupation Title	Unloaded Wage	Loaded Wage
		a	b = a × 1.48
Cybersecurity Coordinator	11-3021 Computer and Information Systems Managers	$71.50	$105.82
Cybersecurity Operations Manager	11-3021 Computer and Information Systems Managers	$71.50	$105.82
Cybersecurity Analyst	15-1240 Database and Network Administrators and Architects	$42.67	$63.15
Attorney	23-1011 Lawyers	$49.11	$72.68
Accountable Executive	11-1011 Chief Executive	$90.75	$134.31

Note: Values rounded to hundredth decimal place unless otherwise displayed.

2.3.4 Pipelines Compensation

For all pipeline owner/operators, TSA uses NAICS 486000 – Pipeline Transportation as the

[150] BLS. May 2022 National Industry-Specific Occupational Employment and Wage Estimates. NAICS 485000 – Transit and Ground Passenger Transportation. Accessed May 1, 2023. https://www.bls.gov/oes/2022/may/naics3_485000.htm

universe from which to pull the occupation-specific base wage.[151] The result for each job title is shown in Table 2-7.

Table 2-7: Associated Labor Rates for Employees in the Pipeline Industry

Job Title	Occupation Title	Unloaded Wage	Loaded Wage
		a	b = a × 1.48
Cybersecurity Coordinator	11-3021 Computer and Information Systems Managers	$79.79	$118.09
Cybersecurity Operations Manager	11-3021 Computer and Information Systems Managers	$79.79	$118.09
Cybersecurity Analyst	15-1212 Information Security Analyst	$47.97	$71.00
Network and Computer Systems Administrator	15-1244 Network and Computer Systems Administrator	$41.36	$61.21
All Pipeline Cyber Positions	15-0000 Computer and Mathematical Occupations	$45.57	$67.44
Audit Manager	11-3012 Administrative Services Managers	$93.31	$138.10
All Pipeline Employees	00-0000 All Occupations	$46.84	$69.32
Administrative Assistant	43-6010 Secretaries and Administrative Assistants	$27.45	$40.63
Attorney	23-1011 Lawyers	$189.33	$280.21
Accountable Executive	11-1011 Chief Executive	$180.61	$267.30
Physical Security Coordinator	11-0000 Management Occupations	$88.00	$130.24

Note: Values rounded to hundredth decimal place unless otherwise displayed.

2.3.5 Modal Compensation Summary

As discussed throughout Section 2.3, TSA utilizes BLS data to determine fully-loaded wage rates across the modal populations.[152] Table 2-8 presents a summary of estimated loaded wage rates for key job titles used in the analysis for each mode.

[151] BLS. May 2022 National Industry-Specific Occupational Employment and Wage Estimates. NAICS 486000 – Pipeline Transportation. Accessed May 1, 2023. https://www.bls.gov/oes/2022/may/naics3_486000.htm

[152] Note that not all requirements apply to OTRB, thus, the wages for only those job titles that would be affected are shown.

Table 2-8: Loaded Wage Rates by Mode

Job Title	Occupation Title	Freight Loaded Wage	PTPR Loaded Wage	OTRB Loaded Wage	Pipeline Loaded Wage
Cybersecurity Coordinator	11-3021 Computer and Information Systems Managers	$127.10	$105.82	$105.82	$118.09
Cybersecurity Operations Manager	11-3021 Computer and Information Systems Managers	$127.10	$105.82	$105.82	$118.09
Cybersecurity Analyst	15-1240 Database and Network Administrators and Architects	$67.34	$63.15	$63.15	$71.00
Network and Computer Systems Administrator	15-1244 Network and Computer Systems Administrator	$64.63	$63.63		$61.21
All Cyber Positions	15-0000 Computer and Mathematical Occupations	$97.28	$71.26		$67.44
Audit Manager	11-3012 Administrative Services Managers	$92.65	$60.44		$138.10
All Employees	00-0000 All Occupations	$53.19	$31.23		$69.32
Administrative Assistant	43-6010 Secretaries and Administrative Assistants	$40.42	$30.07		$40.63
Attorney	23-1011 Lawyers	$130.21	$72.68	$72.68	$280.21
Accountable Executive	11-1011 Chief Executive	$202.60	$134.31	$134.31	$267.30
Physical Security Coordinator	11-0000 Management Occupations				$130.24

Note: Values rounded to hundredth decimal place unless otherwise displayed.

2.3.6 TSA Compensation

Ensuring compliance with many of the provisions of the rule would require consultation with, and review by, a variety of TSA personnel. TSA leveraged the General Schedule pay scale as a proxy to derive the fully-loaded equivalent TSA wage rates.[153] To derive fully-loaded wages, TSA accounted for Special Act Awards and Annual Performance awards, overtime, personnel compensation benefits, and metro travel reimbursements. [154] Pay bands are consistent across job titles. For example, a J-band inspector is paid the same wage as a J-band analyst. The results for

[153] U.S. Office of Personnel Management (OPM). Policy, Data, Oversight: Pay & Leave. Salary Table 2022-DCB. https://www.opm.gov/policy-data-oversight/pay-leave/salaries-wages/. Accessed on July 7, 2023. TSA uses the GS scale as a proxy as it is more widely recognized and available than TSA's separate governmental wage rates.

[154] TSA uses DHS 2022 Modular Cost Model data to load wages to reflect the sum of all Personnel Compensation and Benefits for the corresponding pay scale. TSA added 1.5 percent of the corresponding GS annual base salary to the unloaded annual salary to include both Special Act Awards and Annual Performance Awards. In addition, TSA added an average of 52 hours of overtime to the base unloaded annual salary for GS 9, 11, and 12 positions, as well as 1 percent bonus, 30.2 percent personnel compensation benefit, and a metro travel reimbursement equivalent to $3,120 for each unloaded annual salary.

TSA are shown in Table 2-9. For purposes of this analysis, TSA is using the Washington-Baltimore-Arlington-DC-MD-VA-WV-PA locality for all affected personnel but recognizes that employees may be located in regional offices across the country. Although this is a higher cost locality (5th out of 53 locality areas), TSA anticipates many of the activities identified in the rule would be based out of TSA headquarters in DC (especially in Year 1). In addition, TSA expects most reviewers and inspectors, if not located in DC, to be located in metropolitan areas with higher locality percentages as well (similar to DC).

Table 2-9: Associated Labor Rates for TSA Employees

Pay Band	GS Scale	Annual Unloaded Salary	Additional Pay and Benefits	Loaded Annual Salary	Loaded Hourly Wage Rate
		a	b	c = a + b	d = c ÷ 2,087 hours
H-Band	GS 9,11,12, Step 3 Avg	$80,615.33	$32,004.43	$112,619.76	$53.96
I-Band	GS 13 Step 3	$113,944.00	$154,323.69	$268,267.69	$73.96
J-Band	GS 14 Step 3	$134,649.00	$181,799.22	$316,448.22	$87.11
K-Band	GS 15 Step 3	$158,383.00	$213,294.24	$371,677.24	$102.20
Blended 2 x I-band, 2 x J-Band					$80.54

Note: Values rounded to hundredth decimal place unless otherwise displayed

In many instances, the actions taken by TSA would span across multiple bands. In such situations, TSA calculates a blended, or weighted average, wage based on the number of hours performed by each pay band. However, TSA estimates many tasks identified in response to the proposed rule would be covered equally by both an I- and a J-band employee. To that end, TSA estimates a blended wage rate of $80.54 per hour to represent the average compensation rate using the wage rate of $73.96 for I-Band employees and of $87.11 for J-band employees that can be applied when the estimated hours is equally distributed between the bands (i.e., 50/50 split).

2.4 Rule Provision Unit Costs and Assumptions

The time burdens estimated for each provision were derived in consultation with internal TSA subject matter experts. TSA invites comment on the estimate of the time it would take to fully address and comply with the provisions detailed throughout Section 2. However, TSA recognizes implementation of best practices for cybersecurity risk management programs are both highly individualized for each entity and regularly evolving with changing technology and shifting strategies to combat new threats. Further, it is understood that many individual cybersecurity practices are confidential and not shared publicly, due to both the potential inclusion of proprietary trade information and technology as well as to reduce information that could be viewed by nefarious actors as to existing vulnerabilities. Due to these factors, there is a lack of empirical data to estimate the burden for implementing these requirements. In response, TSA uses a combination of industry experts, cybersecurity policy experts, and TSA compliance knowledge to estimate average burdens and costs where data are insufficient. TSA subject matter experts develop input values based on their professional experience, training, and existing industry relationships. When TSA presents a range of hours, the midpoint is generally chosen; however, there are provisions where TSA believes entities would incur costs at the lower or higher end of the range based on institutional knowledge and stakeholder communications and selects a representative estimate. Nonetheless, TSA also welcomes public comment that provides additional input on the time or cost burdens that would be incurred by those impacted by the rulemaking. Comments that will provide the most assistance to TSA will reference a specific portion of this proposed rule, explain the reason for any suggestion or recommended change, and include data, information, or authority that supports such suggestion or recommended change.

2.4.1 Familiarization

TSA assumes all owner/operators would first spend time determining if the rule applies to them. To do so, TSA anticipates an individual with the equivalent responsibility of the accountable executive and an attorney would each spend an average of 0.5 hours each in Year 1 reviewing the applicability sections of the proposed rule in order to make such a determination.

For those to whom the rule applies, or affected owner/operators, they would incur additional costs to understand the requirements of the rule and their obligations to be in compliance. TSA estimates that a cybersecurity operations manager (COM) and attorney from each affected owner/operator across all modes would each spend 7.08 hours in Year 1 (per occupation) to review the regulation (and in subsequent years only for new entrants). TSA calculates the time necessary for this review based on the number of words in the NPRM and associated RIA sections divided by an average number of words read per minute estimate.[155] On top of the estimated time burden to review the regulation, TSA estimates that an additional 30 minutes of time will be taken for a COM to brief an accountable executive on the requirements of the rule (15 minutes for the COM to give the brief and 15 minutes for the accountable executive to receive the brief).

2.4.2 Form, Content, and Availability of CRM program

This provision details the components covered entities would be required to have in their CRM

[155] TSA assumes each security coordinator and accountable executive would read the NPRM, the cross modal section of the RIA, and only review their specific modal's portion of the RIA. TSA assumes the number of words, at the time of this analysis, in the NPRM and the RIA in order to perform this calculation. TSA assumes the coordinator and accountable executive read at a rate of 238 words per minute. 7.08 hour familiarization time = ((81,503 words in CRM NPRM + (78,358 words in CRM RIA and cross modal section × 25%)) ÷ 238 words per minute ÷ 60 minutes. Source: "How many Words do we read per minute?" by Marc Brysbaert. (https://www.researchgate.net/publication/332380784_How_many_words_do_we_read_per_minute_A_review_and_meta-analysis_of_reading_rate).

programs. These include a cybersecurity evaluation (CSE), a TSA-approved Cybersecurity Operational Implementation Plan (COIP), and a Cybersecurity Assessment Plan (CAP). Also specified in this section are the parameters for 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 detailed in the regulatory text must clearly identify and distinguish application of the requirements to each business unit. The coverage and cost impacts of the provisions that make up the required content of the CRM program are detailed in subsequent sections of this RIA.

2.4.3 Cybersecurity Evaluation (CSE)

This provision requires that each owner/operator who is required to have a CRM program to complete an initial and recurrent cybersecurity evaluation (CSE).[156] The evaluation needs to be sufficient to determine the owner/operator's current enterprise-wide cybersecurity profile of logical/virtual (i.e., software-based techniques) and physical security controls when compared to CRM program requirements to determine their overall cybersecurity posture.[157] It is expected that this evaluation would involve an assessment of the feasibility of current practices and activities to address cybersecurity risks to Owner/Operators Information and Operational Technology systems against their policies or other state/federal regulation or guidelines (e.g. NIST Cybersecurity Framework, Cybersecurity Performance Goals, TSA Pipeline Security Guidelines March 2018 with April 2021 revision). The evaluation would also look at identifying any gaps or

[156] § 1580.305 Freight Rail Transportation Security Cybersecurity Evaluation, § 1582.205 Public Transportation and Passenger Railroad Security Cybersecurity Evaluation, and § 1586.205 Pipeline Facilities and Systems Security Cybersecurity Evaluation

[157] For purposes of this analysis, logical/virtual relates to the software-based techniques as they relate to authentication, that include but are not limited to usernames and passwords, two-way authentication, and token security while physical security relates to the protection of equipment and sites from in-person intruders, natural disasters, vandalism, and other types of damage.

vulnerabilities against security controls from NIST 800-53 and 800-82. Such security controls include alignment to Assets Management, Controls Management, Configurations Management, Vulnerability Management, and Training & Awareness. The CSE would also identify remediation measures that will be taken to address those gaps which could include upgrading software/hardware/systems or removing access. The CSE can be facilitated using a TSA provided form or other tools approved by TSA. TSA anticipates that owner/operators would be able to utilize existing tools, such as the Cybersecurity Assessment Tool (CATT) and/or the TSA Cyber Security Evaluation Tool (CSET) platform to aid in conducting this evaluation.[158] The CSE would recur annually and TSA SMEs estimate a cybersecurity analyst would spend 30 hours undertaking this evaluation with an additional 10 hours of network/systems engineer time for a total burden of 40 hours per year for freight and PTPR. For pipeline, due to the nature of the industry, this evaluation is expected to take 120 hours. This evaluation would recur annually and TSA SMEs estimate a cybersecurity analyst would spend 90 hours undertaking this evaluation with an additional 30 hours of network/systems engineer time for a total of 120 burden hours per year. Across all modes, TSA expects the time burden to remain constant year to year as it assumes affected owner/operators would conduct a full evaluation annually given continually changing technology and threats (the evaluation would not be based on static parameters) but requests public comment on this assumption.

As a result of this evaluation, TSA anticipates that all owner/operators would work to address identified risks and vulnerabilities and that the majority are likely to resolve these issues as part of their COIP. However, TSA estimates that 20 percent of owner/operators would spend 40

[158] The platform is a free tool and can be accessed by visiting tsa-download.inl.gov.

hours annually to take immediate action to address identified risks and vulnerabilities. An example would be revising an existing process or planning for the replacement of equipment or software that is outdated or reached the end of its useful life. TSA assumes that immediate mitigation actions would focus on items that would occur within existing systems and that capital outlays, such as new software or firmware, that may be identified during the CSE process would be allocated for during the longer-term COIP implementation. TSA requests comment on the makeup of actions undertaken during this mitigation period, specifically, if such immediate actions would focus mainly with existing systems or if items such as new or additional software or firmware would be acquired. As the CSE recurs annually, TSA estimates the cybersecurity analyst and network/systems engineer would each spend an average of 20 hours annually (evenly split to account for immediacy and complexity of tasks) addressing identified vulnerabilities and risks for a total burden of 40 hours per year.

TSA would also incur costs. TSA SMEs estimate they would spend 4 hours annually processing each owner/operator's evaluation.

2.4.4 Cybersecurity Operational Implementation Plan (COIP)

This provision requires the development and submission of a Cybersecurity Operational Implementation Plan (COIP) which represents the cornerstone of a comprehensive CRM program. The COIP lays out the owner/operator's plan relating to physical and logical/virtual security controls, and how they would comply with the requirements of this proposed rule in order to mitigate the threats associated with potential cybersecurity attacks. The COIP is to include general information (e.g., owner/operator contact information and plan applicability) as well as specific content on: 1) Governance, 2) Identification of Crucial Cyber Systems, Network Architecture, and Interdependencies, 3) Procedures, policies, and capabilities to protect Critical

Cyber Systems, 4) Procedures, policies, and capabilities to detect cybersecurity incidents, and 5) Procedures, policies, and capabilities to respond to, and recover from, cybersecurity incidents. Furthermore, owner/operators would also be required to provide a Plan of Action and Milestones (POAM) for areas that they determine do not yet have measures in place to meet identified security outcome requirements as specified in the regulatory text sections associated with this provision for each mode.[159] The costs estimates associated with each of the COIP elements are provided in subsequent sections.

However, the hourly burden to TSA, as it relates to the COIP, includes 50 hours in Year 1 to review the COIP. TSA also estimates legal consultation and review would be necessary in 50 percent of owner/operator submitted COIPs to address a specific issue or topic, and not the entirety of the COIP, which TSA estimates as taking 4 hours per COIP. Further, TSA would incur training costs associated with federal employees evaluating owner/operator submitted COIPs. TSA estimates approximately 100 TSA employees would spend 40 hours each quarter of the first three years of the period of analysis on this effort (for a total of 160 hours per year), with the time burden dropping to 40 hours annually after Year 3, as the program matures and moves from the initial ramp up and learning what will be needed for COIP review to a steadier state with a greater focus on COIP revisions. TSA also anticipates it would take 5 employees 100 hours each to develop this training (500 hours total) in Year 1. In Years 2-3, this time burden decreases to 50 hours per employee (250 hours total) and in year 4 and beyond, the burden would drop to 20 hours per employee (100 hours total). Similar to the decrease in needed training time,

[159] § 1580.307 Freight Rail Transportation Security Cybersecurity Operational Implementation Plan, § 1582.207 Public Transportation and Passenger Railroad Security Cybersecurity Operational Implementation Plan, and § 1586.207 Pipeline Facilities and Systems Security Cybersecurity Operational Implementation Plan

the development time associated with training will also decrease as the program matures, support materials such as standard operating procedures are developed, and focus shifts on accounting for incremental COIP changes.

2.4.4.1 Governance

As it pertains to governance of the CRM program, each affected owner/operator must designate an accountable executive to ensure there is cohesion and authority across the various parts of the CRM program with individuals who are fully versed in the content as well as their obligations. Specifics relating to those designations are further detailed in the respective regulatory text sections.[160] TSA expects individual(s) responsible for the governance and sustainment of the company's cybersecurity program would have final approval on program parameters and that this person would be at an executive level. TSA estimates that each owner/operator would spend three hours making this determination, split between one hour of COM time to make the designation and two hours of attorney time to review and document the qualifying criteria for determining an accountable executive. TSA also accounts for turnover based on rates detailed in Table 2-1 above where this designation would need to be updated due to employment changes.

In addition, TSA estimates each affected owner/operator would spend 40 hours, on average, in Year 1 to review the requirements involved in the COIP, provide necessary information, and compile specific content materials into the COIP. TSA SMEs with expertise in cybersecurity estimate the hour burden would take 40 hours for this facet of the COIP requirements due to the complexities and system areas involved and that there would be both legal as well as technical

[160] § 1580.309 Freight Rail Transportation Security Governance of CRM Program, § 1582.209 Public Transportation and Passenger Railroad Security Governance of CRM Program, and § 1586.209 Pipeline Facilities and Systems Security Governance of CRM Program.

review to determine what is needed to meet the requirements. TSA estimates such efforts would be evenly split between a COM and a corporate attorney. While there is no mandated time period for when or how frequently the COIP must be updated, TSA assumes that owner/operators are reviewing their COIPs regularly and updating in response to other requirements. For years 2-10, TSA assumes owner/operators would spend 40 hours, in any one year in a three-year period, which TSA presents as an annual average of 13.3 hours, as a representative frequency for updates. This time would encompass both review time as well as the time to incorporate any identified revisions. Additionally, as the COIP is a security program, owner/operators must request an amendment whenever they seek to make substantive changes to their COIPs. 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. Amendments would not be required for technical, i.e., administrative or clerical changes to COIPs. Substantive changes requiring an amendment would include (but are not limited to) items such as 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; updates to risk methodologies; and other such actions. As the frequency and complexity of these amendments, in relation to regular COIP updates, is unknown, TSA has not quantified their cost in this analysis; but recognizes it may result in additional burden from time spent to develop and implement.

As there is a wide variation in entity systems and complexities, TSA developed an estimated range of how long developing and implementing the required COIP provisions may take owner/operators. The range values are discussed throughout this section, along with the data value estimate TSA is using in its calculations.

2.4.4.2 Cybersecurity Coordinator

The rule requires the designation of a cybersecurity coordinator and alternate and for the owner/operator to report those individuals' contact information to TSA.[161] The coordinator and alternate must be U.S. citizens eligible for a security clearance, unless otherwise waived by TSA, and both the coordinator and alternate must have the requisite experience within the cyber security profession, and be available to contact or be contacted by TSA 24 hours a day and 7 days a week. The cybersecurity coordinator serves as the designated TSA point of contact and these qualification requirements are to ensure the person is trained and knowledgeable enough to quickly and accurately engage with TSA when needed. The qualifications of the cybersecurity coordinator must be reviewed by the company to determine they meet the requirements of the role. TSA estimates owner/operators would have one person filling this role. TSA also estimates that owner/operators would have one person filling the role of alternate and that the employee turnover rate would apply to every affected owner/operator.

TSA estimates each entity would spend a total of two hours reviewing and determining the cybersecurity coordinator and alternate. The two hours is a per designated individual estimate and the breakout includes 15-minutes each for the coordinator and alternate to be designated by

[161] § 1580.311 Cybersecurity Coordinator, § 1582.211 Cybersecurity Coordinator, § 1586.211 Cybersecurity Coordinator

the COM and 45-minutes each for an individual with the equivalent responsibility of the cybersecurity coordinator to submit the coordinator and alternate information and one hour each for an attorney to review.

Based on its experience with the Security Directives, TSA estimates it would spend 1 hour per designated individual to receive and review the coordinator information, have any needed discussion, and record entries.

2.4.4.3 Identification of Critical Cyber Systems

Identification of Critical Cyber Systems includes providing a list of Critical Cyber Systems, as defined in the TSA Cybersecurity Lexicon, including relevant characteristics (e.g., system name and manufacture), a description of the methodology used which considers a number of identified factors (e.g., critical functions, operational impacts, system vulnerabilities and interdependencies, and likelihood of attack), and critical system network architecture information (e.g., external connections, zone boundaries, and acceptable communications).[162] This provision focuses on the review of cyber systems and determining their level of criticality which helps inform what security measures may be warranted. This represents a more detailed investigation into one aspect of cybersecurity as compared to the broader CSE which looks company-wide at the entity's cybersecurity posture.

TSA estimates affected entities would spend an average of 160 hours in Year 1 performing these

[162] § 1580.313 Identification of Critical Cyber Systems, § 1582.213 Identification of Critical Cyber Systems, § 1586.213 Identification of Critical Cyber Systems

tasks and 40 hours in subsequent years (Years 2 through 10) to review and update.[163] In Year 1, TSA SMEs with information technology expertise estimate these 160 hours would capture designing the criteria, conducting an IT and OT inventory, creating a database, keeping it up to date, and integrating criticality designations. TSA notes that, for affected rail systems, this proposed rule would require rail owner/operators who use PTC to include specific PTC components as Critical Cyber Systems and estimates this would be completed within the overall time burden allocated. TSA estimates these tasks will be split between the COM (50 percent), network/systems administrator (20 percent), and a cybersecurity analyst (30 percent). For Years 2 through 10, TSA assumes there would be some efficiency gains from experience implementing these processes but retain the same split between occupations.

2.4.4.4 Supply Chain Risk Management

Under the proposed rule, owner/operators must incorporate into their COIP policies, procedures, and capabilities to address supply chain cybersecurity vulnerabilities. This includes ensuring all procurement documents and contracts include a requirement for the vendor or service provider to notify the owner/operator of cybersecurity incidents, vulnerabilities, and an evaluation of the cybersecurity measures implemented by vendors. In addition, owner/operators must consider the level of cybersecurity sufficient to protect against or respond to cybersecurity incidents and mitigation measures to address risks identified by the vendor or service provider. The cost of this requirement includes the time incurred for contract renewals and updates to come into compliance, as well as the time owner/operators spend to check the goods, services, or

[163] TSA consulted SMEs with cybersecurity expertise and determined that an hour burden range of 80 – 240 hours for Year 1 and a range of 40 – 120 hours for Years 2-10. TSA uses the midpoint of 160 hours for Year 1 and the low end of the range, or 40 hours, for Years 2-10 as TSA SMEs believe it better reflects the average cost incurred by owner/operators.

capabilities provided by vendors or service providers to identify potential vulnerabilities. TSA estimates affected entities would spend an average of 330 hours annually to perform these tasks. This includes 10 hours of attorney time to review and update contracts and 40 hours for a team of 4 individuals to check vendor provided capabilities twice a year.[164] TSA SMEs with cybersecurity expertise estimate checking vendor-provided capabilities would be split between a COM who would incur a time burden of 160 hours, a cybersecurity analyst who would incur 112 hours of time, and a network/systems administrator who would incur 48 hours of time. As affected owner/operators incorporate security elements into their contracts, TSA anticipates such vendors may incur additional costs to meet such requirements if they do not do so already. However, such measures or additional provisions would likely become standard business practices to remain competitive in the field.

2.4.4.5 Protection of Critical Cyber Systems

To meet the protection requirements needed in the COIP, owner/operators would develop and implement network segmentation policies between OT and IT. [165] TSA SMEs estimate affected entities would spend, on average, 820 hours in Year 1 and 660 hours in Years 2 through 10 performing this task. This 820-hour total time estimate in Year 1 is comprised of 100 hours to design the individual criteria for network segmentation policies, 120 hours to conduct an inventory of OT (which involves an asset inventory to create a comprehensive list of all OT within the organization), 120 hours to review OT to OT connections, 120 hours to review OT to IT connections, 120 hours to review OT connections to third parties, and 240 hours to develop

[164] TSA estimates four (4) cybersecurity analysts would spend 40 hours twice a year. 4 analysts × 40 hours × 2 times a year = 320. 320 hours for the cybersecurity analysts + 10 hours for an attorney = 330 hours.

[165] § 1580.317 Freight Rail Transportation Security Protection of Critical Cyber Systems, § 1582.217 Public Transportation and Passenger Railroad Security Protection of Critical Cyber Systems, § 1586.217 Pipeline Facilities and Systems Security Protection of Critical Cyber Systems

networking solutions to ensure OT and IT are separate. For Years 2 through 10, TSA assumes each of the above tasks would continue each year, with the application components burden remaining constant and the time to design the criteria dropping by 40 percent to 60 hours and the time to design networking solutions to keep IT and OT separate dropping by 50 percent to 120 hours, for a total ongoing annual burden of 660 hours. TSA assumes these tasks would be undertaken by the equivalent of a COM, system/network administrator, and a cybersecurity analyst. As the time involved on this task may vary across owner/operators within a mode as well as across industries, TSA requests comment on the burden hour estimates.

In order to secure and prevent unauthorized access to Critical Cyber Systems, owner/operators would also implement access control measures (e.g., password reset schedule, multi-factor authentication, policies and procedures for access rights management, standards for not allowing or limiting use of shared accounts, schedule for reviewing domain trust relationship).[166] In consultation with SMEs with cybersecurity experience, TSA estimates a potential range for owner/operators of 75 hours to 200 hours for owner/operators to perform this task. TSA SMEs expect that most owner/operators' time would be towards the lower end of the range and thus estimates 100 hours in Year 1 and 58.34 hours in Years 2 through 10.[167] However, TSA recognizes that some owner/operators may require more or less time to accomplish the stated objectives. The Year 1 breakdown is 50 hours to design the criteria, 33.33 hours to conduct an access review, and 16.67 hours to design network solutions.[168] The 33.33 hours needed for access

[166] § 1580.317 Freight Rail Transportation Security Protection of Critical Cyber Systems, § 1582.217 Public Transportation and Passenger Railroad Security Protection of Critical Cyber Systems, § 1586.217 Pipeline Facilities and Systems Security Protection of Critical Cyber Systems

[167] TSA included a large range to account for individual entity variations but anticipates more entities would incur costs at the lower end and thus uses an estimated average of 100 hours in Year 1.

[168] The time to conduct an access review is estimated to be a third of the overall 100-hour burden, while the time to design networking solutions is estimated to be a sixth of the overall 100-hour burden.

review continues unchanged in Years 2 through 10 while the ongoing burden for designing the criteria and designing the network solutions drops to 16.67 and 8.34 hours, respectively.[169] TSA assumes these tasks would be undertaken by the equivalent of a network/systems administrator, cybersecurity analyst, and the COM.

In addition, TSA estimates an annual multi-factor authentication unit cost of $72 per employee ($6 per user per month for the required software) as a representative average, but acknowledges that some companies may incur a higher or lower cost per employee.[170] In addition, TSA estimates that each employee would spend 4.17 hours annually using multi-factor authentication (1 minute per day per employee).[171] TSA assumes employees would use MFA daily to log into IT network systems such as email, chat communications, file share servers, or HR systems. Since these are systems employees engage with regularly, TSA estimates that account lockouts will be rare. Furthermore, TSA estimates there would be an additional time burden for resolving lockouts and password resets of 3 hours assuming each lockout takes 15 minutes to resolve and an occurrence of twice every 2 months per employee.[172] Together, TSA calculates each employee

---

[169] To derive the time needed in Years 2-10, TSA assumes that the time to design criteria will be 30 percent of the time needed in year 1, resulting in a burden of 16.67 hours. TSA assumes the time needed for access review will remain unchanged in years 2-10, while the time to design networking solutions will be 50 percent of the time needed in year 1, resulting in a burden of 8.34 hours. This results in a total access control time burden of 58.34 hours in years 2-10.

[170] TSA relies upon data from Microsoft Azure's Pricing Calculator for the estimate of $72 per person annually for MFA software. "Azure Active Directory Pricing Calculator." Microsoft Azure. https://azure.microsoft.com/en-us/pricing/calculator/.

[171] TSA estimates 1 min per day per employee to access MFA for a total hour burden of 4.17 hours per year, per employee. (60 seconds) × 250 working days per year = 4.17 hours. 250 working days per year excludes weekends and Federal holiday (365 days per year – (52 weeks in a year x 2 weekend days per week) – 11 Federal holidays.

[172] TSA relies upon data from Microsoft's Security Center default settings for the estimate of 15 minutes per lockout and PCMag regarding the estimated number of lockouts expected per employee per year. "Account Lockout Policy." Microsoft 365. May 11, 2023. https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/account-lockout-policy. Accessed on July 14, 2023. See also, Griffith, Eric. "Average US Internet User is Locked Out of 10 Accounts per Month." PCMag. April 13, 2021. https://www.pcmag.com/news/average-us-internet-user-is-locked-out-of-10-accounts-per-month. Accessed on July 14, 2023.

incurs a time burden of 7.17 hours per year per employee due to MFA requirements.

Furthermore, each owner/operator must develop a patch management strategy that ensures all critical security patches and updates for operating systems, applications, drivers and firmware are current.[173] The strategy would be required to include the following:

- The risk methodology for categorizing and determining criticality of patches and updates;
- An implementation timeline based on categorization and criticality; and
- Prioritization of all security patches and updates on CISA's Known Exploited Vulnerabilities Catalog.

TSA estimates affected entities would spend 82 hours in Year 1 and 80 hours in Years 2 through 10 performing this task. This time breakdown includes time spent to create and maintain a patch management strategy; TSA believes the average time owner/operators would spend undertaking these actions is 4 hours in Year 1 and 2 hours in subsequent years. Owner/operators would also incur 78 hours each year to manage new patches which entails researching and learning about available patches by spending 1.5 hours per week consulting CISA's Known Exploited Vulnerabilities Catalog. TSA assumes the 78 hours would be a static burden estimate and that the above tasks would be managed by a system/network administrator and the COM.

Owner/operators would also incur a time burden responding to new patches. In general, due to the complexity of resources and time needed for deployment, patching occurs during

[173] § 1580.317 Freight Rail Transportation Security Protection of Critical Cyber Systems, § 1582.217 Public Transportation and Passenger Railroad Security Protection of Critical Cyber Systems, § 1586.217 Pipeline Facilities and Systems Security Protection of Critical Cyber Systems

owner/operator downtime or because of a major event. TSA believes that the requirements set forth in this proposed rule would result in more frequent and comprehensive patching. TSA estimates an average of one additional patch cycle per quarter and that it would take 375 hours to complete each cycle for a total of 1,500 hours.[174] This estimate includes time to evaluate and test patches, as well as scheduling and pushing out the necessary patches to affected equipment. TSA assumes this task would be overseen by a system/network administrator. TSA recognizes that patch frequency could vary amongst owner/operators with cycles as frequent as one patch cycle per month (or 12 each year) and requests public comment on the average patch cycle frequency.

Finally, the cost of data backups for Critical Cyber Systems includes the cost to backup all Critical Cyber System data and the time burden to supervise the backup process. Industry best practices regarding backup protocols vary widely and will be dependent on multiple factors, including entity size and business needs. The point estimates on data volume and backup frequency represent an approximate average across the covered entities and modes. TSA cybersecurity SMEs estimates an average Critical Cyber System data volume per entity per backup in Year 1 of 500 terabytes (TB) of data. TSA estimates the cost per TB of data backed up as $329.16 per TB.[175] TSA estimates that the network systems administrator would spend 12 hours per year (one hour per month) to supervise the backup of their Critical Cyber System data. Upon completion of the backup, the data must be securely stored. As with the amount of data

---

[174] TSA SMEs with cybersecurity expertise estimate that this component would have an hour burden ranging from 250-1250 in Years 1-10. TSA decided to use an hour burden of 375 hours to reflect that a few covered entities would have hour burdens significantly higher than the rest due to their size.

[175] "Cloud Storage Pricing in 2023: Everything You Need to Know." Anina Ot. Accessed September 26, 2023. https://www.enterprisestorageforum.com/cloud/cloud-storage-pricing/. TSA uses the above article's "Cloud Storage Pricing Chart" to compare five of the six (U.S.-based) cloud storage providers. The table's final row provides a per month per TB cost estimator. The article's five point estimates average to $27.43 per TB per month (($34.67 + $24.90 + $24.08 + $26.40 + $27.00) / 5). TSA multiplies the per month amount by 12 months to yield an annual cost of $329.16 per TB per year.

and backup frequency, the length of time needed to store a backup varies greatly and can range from 90 days to 3 years depending on the type of data and owner/operator priorities. Additionally, many of the covered owner/operators hold cybersecurity insurance policies, which would come with their own requirements on data storage and protection of critical systems. While these policies may be in place, there would be a wide range in terms of what is required by each carrier to ensure full compliance with the provisions of the rule.

2.4.4.6 Procedures, Policies, and Capabilities to Respond to, and Recover from, Cybersecurity Incidents.

Each owner/operator must ensure that its COIP includes policies, procedures, and capabilities sufficient to detect and respond to cybersecurity threats to, and anomalies on, Critical Cyber Systems.[176] At minimum, they must be able to defend against malicious email, block suspicious ingress and egress communications, control the impact of known or suspicious web domains and applications, block and defend against unauthorized code, monitor and/or block connections from known or suspected malicious command and control servers, and ensure continuous collection and analysis of data on Critical Cyber Systems and other directly connected IT and OT systems. TSA expects that these policies and procedures would be undertaken as part of the overall CRM development.

2.4.4.7 Cybersecurity Training

The proposed rule requires two types of training, basic cybersecurity training and role-based

[176] § 1580.323 Capabilities to respond to a cybersecurity incident, § 1580.325 Reporting cybersecurity incidents, § 1580.327 Cybersecurity Incident Response Plan, § 1582.223 Capabilities to respond to a cybersecurity incident, § 1582.225 Reporting cybersecurity incidents, § 1582.227 Cybersecurity Incident Response Plan, § 1586.223 Capabilities to respond to a cybersecurity incident, § 1586.225 Reporting cybersecurity incidents, § 1586.227 Cybersecurity Incident Response Plan

cybersecurity training, as specified in the regulatory text.[177] Affected entities would be required to train employees in cyber security measures to safely interact with their computer networks and on the internet with more rigorous requirements for employees with access to sensitive components of their owner/operator's network. To derive the employee populations, TSA first reviewed the overall total industry population for each modal NAICS code in BLS OEWS data. From there, TSA SMEs estimate that owner/operators covered by the scope of this rule represent approximately 80 percent of the industry wide employee population. From that universe, TSA assumes that all employees would receive basic user awareness training and 15 percent would also receive role based cybersecurity training. Owner/operators would also be required to submit training curriculum to TSA for approval and retain training records.

Basic User Awareness Training would be required of all employees, including contractors with access to the owner/operator's Information or Operational Technology systems.[178] Such training is intended to help employees understand proper cyber-hygiene and the security risks associated with their actions. Training modules would include as proposed in the regulatory text:

- Social Engineering, including phishing;
- Password best practices;
- Remote work security basics;
- Safe internet and social media use;

[177] § 1580.319 Cybersecurity training and knowledge, § 1582.219 Cybersecurity training and knowledge, § 1586.219 Cybersecurity training and knowledge

[178] To estimate this population, TSA utilizes BLS Employment Projections and OEWS data Based on the NAICS code for each mode to extract employment and wage information for Occupation 00-0000 All Occupations.

- Mobile device (wireless) vulnerabilities and network security;

- Data management and information security, including protecting business email, confidential information, trade secrets, and privacy; and

- 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. Recurrent training would be required every year. TSA estimates each employee would spend, on average, one hour per year completing this training.

Role-based cybersecurity Training would be provided to cybersecurity-sensitive employees that specifically addresses their role as a privileged user to prevent and respond to a cyber-incident, acceptable uses, and the risks associated with their level of access and use as approved by the owner/operator. A privileged user is one user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.[179] TSA estimates each such designated employee would spend 2 hours completing this specialized training which would need to be completed annually.

Curriculum Development would be required of each owner/operator specific to their IT systems and/or operational environments. TSA expects training modules would include topics proposed in the regulatory text such as:

[179] TSA identifies this population based on BLS Employment Projections and OEWS data. Within the NAICS code for each mode, TSA extracts out employment and wage information for Occupation 15-0000 All Computer and Mathematical Occupations.

- 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;

- Recognition and detection of cybersecurity threats, types of cyber incidents, and techniques used to circumvent cybersecurity measures;

- Incident handling, including procedures for reporting a cybersecurity incident to the COM and understanding their roles and responsibilities during a cybersecurity incident and implementation of the owner/operators' CIRP as required;

- Requirements and sources for staying aware of changing cybersecurity threats and countermeasures; and

- Operational Technology-specific cybersecurity training for all personnel whose duties include access to Operational Technology systems.

In Year 1, TSA expects all affected owner/operators would create and submit a training plan.[180] TSA estimates it would take approximately 80 hours for the COM to familiarize themselves with the requirements, develop the training plan, and include any back and forth with TSA. Given that the proposed rulemaking is performance based versus prescriptive, there is anticipated to be a high level of engagement and adjustments needed, both for owner/operators with existing plans as well as those creating full training programs. In addition, TSA would spend 40 hours to process training plan submissions and engage in discussions with owner/operators, as needed.

[180] Training submission is part of the COIP review process.

Cybersecurity Training Record Retention would be required for initial and recurrent cybersecurity training records for everyone required to receive cybersecurity training for no less than five years. For each employee training record, TSA estimates that it would take 1 minute (presented as 0.02 hours) for an administrative assistant to compile and preserve these records.

TSA would also incur an additional time burden of 4 hours to inspect the training records. Recognition of prior or established cybersecurity training is permissible and previously provided cybersecurity training may be credited towards satisfying the requirements of this section provided they address the content laid out in the modules.

2.4.4.8 Detection of Cybersecurity Incidents

The rulemaking includes details on additional requirements that owner/operators must include in their COIP policies, procedures, and capabilities when it comes to detecting and responding to cybersecurity threats to, and anomalies on, Critical Cyber Systems.[181] TSA estimates each affected entity would spend, on average, 106.5 hours in Year 1. In Year 1, this includes four hours to design continuous monitoring criteria, eight hours to develop solutions for IT, two hours per quarter to meet to review security threats (done by four network/systems administrators) for an annual burden of 32 hours, and 15 minutes per work day for updates to the list of blocked websites (a total of 62.5 hours per year). TSA recognizes that some owner/operators may incur a higher or lower burden.[182] For Years 2 through 10, TSA estimates there will be efficiency gains from experience implementing these processes and estimates each affected entity would spend

[181] § 1580.321 Detection of cybersecurity incidents, § 1582.221 Detection of cybersecurity incidents, § 1586.221 Detection of cybersecurity incidents

[182] In discussion with internal cybersecurity experts, TSA calculates the estimated time burden as 4 hours + 8 hours + (2 hours × 4 quarters × 4 network/systems administrators) + (15 minutes per day × 250 working days per year) ÷ 60 minutes = 62.5 hours) = 106.5 hours in Year 1.

100.5 hours in Years 2 through 10 performing these tasks. In Years 2 through 10 TSA estimates each affected entity will spend two hours to design the criteria, four hours to develop solutions for IT, and the continuation of the quarterly meetings and daily updates for an annual burden of 100.50 hours. TSA assumes these tasks would be evenly performed by the COM and network/systems administrator. Based on consultation with SMEs, TSA also estimates that the software used for continuous monitoring ranges from $2,000 to $6,000 per year with a primary annual cost estimate of $2,995 per owner/operator for the software necessary for continuous monitoring.[183] While some affected owner/operators may utilize such software, there is wide variation across the industry, and in order to ensure owner/operators are able to meet the full requirements of the rule, such as those in the CAP, it is prudent to include the full cost of this software.

2.4.4.9 Capabilities to Respond to a Cybersecurity Incident

This provision details additional requirements that owner/operators must include in their COIP capabilities when it comes to responding to cybersecurity incidents that affect Critical Cyber Systems. These specifics are discussed in the rulemaking requirements.[184] TSA includes the time necessary to address these requirements in the plan development estimates, which are discussed in Section 2.4.4.

2.4.4.10 Plan of Action and Milestones

If there are requirements and outcomes of the COIP that an owner/operator does not meet, the COIP must also include a plan of action and milestones (POAM). The POAM must include:

---

[183] Keary, Tim. Comparitech. (2023). The Best Network Monitoring Tools & Software of 2023. https://www.comparitech.com/net-admin/network-monitoring-tools/.

[184] § 1580.323 Capabilities to respond to a cybersecurity incident, § 1582.223 Capabilities to respond to a cybersecurity incident, and § 1586.223 Capabilities to respond to a cybersecurity incident

- Policies, procedures, measures, or capabilities that owner/operators would develop or obtain, as applicable, to ensure all requirements and security outcomes as specified in the COIP are met;

- Physical and logical/virtual security controls that the owner/operator would implement to mitigate the risks associated with not fully complying with requirements or security outcomes of the COIP; and

- A detailed timeframe to meet all required outcomes, as well as any mitigating measures that would be implemented pending full compliance with all requirements and security outcomes of the COIP, not to exceed three years from the date of submission to TSA of the COIP.

The POAM must be updated as necessary to address any deficiencies identified during a CSE or CAP that would not be immediately addressed through an update to the COIP. TSA estimates that 20 percent of owner/operators would need a POAM to be included with their COIP (with the remaining 80% expected to be able to comply with the proposed requirements by the effective date(s) as stated in the rule) in the first three years of the rule. While there may be adjustments that need to be made as systems evolve, TSA anticipates most would be able to be resolved within the context of the overall COIP processes. TSA also estimates these owner/operators would spend between 40 and 160 hours with a primary estimate of 80 hours reviewing each needed POAM. This review entails ensuring that the policies, controls, and timeframes in the POAM are feasible and achieve the desired results. TSA estimates a network/systems administrator will spend 48 hours on this task while a cybersecurity analyst will spend 32 hours. The costs associated with addressing the identified mitigations would be resolved as part of an

entity's overall COIP implementation. One method affected owner/operators might put in place to mitigate physical risks would be an action such as posting a guard either at building entrance/exit points or at the door to a restricted area. Another potential mitigation would be to utilize closed circuit television to consistently monitor the status of the physical space or ensure the system has an alarm to alert to intrusion. For potential compensating controls, various access control measures could be implemented that would entail securing local and/or remote access as a method to prevent unauthorized access to critical cyber systems. Additional security actions could include having a schedule for memorized secret authenticator resets that could work in tandem with mitigation measures that will not have password resets that align with the authenticator reset schedule. TSA requests comment on additional types of physical and/or logical/virtual controls that could be implemented to comply with the requirements.

2.4.5 Reporting Cybersecurity Incidents

This provision states that when there is a cybersecurity incident, affected entities would need to report cybersecurity incidents to the CISA. As detailed in the TSA Cybersecurity Lexicon, discussed in Table 6 of the preamble, a reportable cybersecurity incident is defined as a cyber-incident that leads to, or, if still under the covered owner/operator's investigation, could reasonably lead to any of the following:

(1) a substantial loss of confidentiality, integrity, or availability of a covered information system, network, or operational technology;

(2) a disruption or significant adverse impact on the covered owner/operator's ability to engage in business operations or deliver goods, or services;

(3) disclosure or unauthorized access directly or indirectly to non-public personal information

of a significant number of individuals; or

(4) potential operational disruption to other critical infrastructure systems or assets.

When there is a reportable incident, reporting must take place as soon as practical, but no later than 24 hours after the cybersecurity incident is discovered. Reportable incidents could include:

- Unauthorized access of an IT and OT system
- Discovery of malicious software on an Information or Operational Technology system
- Activity resulting in a denial of service to any Information or Operational Technology system
- A physical attack against the owner/operator's network infrastructure
- Any other cybersecurity incident that results in operational disruption to the owner/operators Information or Operational Technology systems or other aspects of the owner/operator's systems or facilities, critical infrastructure or core government functions, or impacts national security, economic security, or public health and safety.

All reports must be made to CISA incident, to streamline and maximize awareness and response. TSA estimates an average number of freight, PTPR, and OTRB cybersecurity incidents by dividing internal reportable cybersecurity incident data by mode by the number of entities covered by the rule in each mode.[185] Specifically, TSA estimates 0.14 expected freight rail

[185] Based on internal TSA data, TSA estimates cybersecurity incidents per year by mode are: Freight Rail, 10 incidents; PTPR, 15 incidents; OTRB, 15 incidents. For purposes of this analysis, TSA assumes that the universe of those entities reporting is a comparable universe to those entities covered by this proposed rule.

cybersecurity incidents requiring reporting a year per owner/operator, 0.44 expected PTPR cybersecurity incidents requiring reporting a year per owner/operator, and 0.21 expected OTRB cybersecurity incidents requiring reporting a year per owner/operator. For pipeline, TSA utilizes internal data, in consultation with SMEs, relating to reportable incidents to estimate 3.48 pipeline reportable cybersecurity incidents per month per owner/operator.[186] Based on conversations with SMEs, TSA estimates it would take 1 hour of time to report a cybersecurity incident, with a half hour attributed to a cybersecurity analyst and a half hour attributable to the COM.

2.4.6 Cybersecurity Incident Response Plan (CIRP)

Each affected owner/operator must develop and maintain a CIRP as part of their COIP to reduce the impacts of a cybersecurity incident that causes, or could cause, operational disruption or significant impacts on business-critical functions.[187] The CIRP must provide specific measures sufficient to promptly identify, isolate, and segregate infected systems, secure and safely maintain backup data and systems, and ensure that Operational Technology systems can be isolated.

TSA estimates that the COM of each affected owner/operator, for each mode, would spend an average of 80 hours in Year 1 to develop the incident response plan and 20 hours in each subsequent year to maintain said plan.

The rule also requires owner/operators to conduct exercises to test the effectiveness of the plan's procedures and personnel responsible for implementing measures, no less than annually. TSA estimates that, on average, this testing would be carried out by a person with the equivalent

[186] This results in an estimated 400 incidents per year.
[187] See sections §1580.327, §1582.227, and §1586.227

responsibility of the COM at an annual time burden of 120 hours but recognizes the time involved could be larger for a more complex system and less for more straightforward systems.[188]

On top of these requirements, the CIRP must be activated each time there is a reportable incident. Non-reportable incidents make up the vast majority of incidents and are not included in the following burden estimate. For those incidents that do meet the reportable threshold, there will be wide range of time needed to respond. Using an average amount of time needed to respond to reportable incidents, spread across incidents designated as small/medium/large, TSA assumes that for each reportable incident, it would take the network/systems administrator and the cybersecurity analyst 160 hours to complete this action. This time burden is split equally between the network/systems administrator and the cybersecurity analyst.

TSA would also incur costs. TSA estimates it would take 4 hours for it to process each owner/operator's CIRP. When there is a reported incident, TSA assumes 10 percent would require an on-site presence and, in consultation with SMEs, estimates this would require 32 hours of TSA time, plus travel and lodging costs. To determine travel and lodging costs, TSA utilizes published GSA per diem rates for the Washington, DC locality based on April 2022 allowances as spring and summer values are higher in order to avoid underestimating cost burdens. The daily lodging rate is $258, Meals and Incidentals is $79 (reduced to $59 on the first and last days of travel). [189] Flight tickets are estimated as $378, based on annual average domestic

[188] Incident Response Planning. Microsoft. https://learn.microsoft.com/en-us/security/operations/incident-response-planning. April 24, 2023. Accessed July 14, 2023.

[189] U.S. General Services Administration. Per Diem Rates. Retrieved from https://www.gsa.gov/travel/plan-book/per-diem-rates/per-diem-rates-results?action=perdiems_report&fiscal_year=2023&state=DC&city=&zip=. Last accessed June 10, 2023.

air fares.[190] While origination and destination locations would vary, TSA is using the Washington, DC locality as a benchmark value in its estimates as discussed in Section 2.3.6.

2.4.7 Cybersecurity Assessment Plan (CAP)

To be in compliance with the requirements of the rulemaking, each affected owner/operator would, no later than 12 months from TSA's approval of the owner/operator's COIP, create and submit to TSA a CAP.[191] The plan would proactively assess the effectiveness of the COIP and identify and resolve device, network, and/or vulnerabilities associated with the Critical Cyber Systems.[192] In order to ensure both the owner/operator and TSA are in agreement on the planned assessment program and that said assessment would fulfill the requirements by the end of the three-year CAP cycle, TSA would require the CAP to include a mapping that would sufficiently validate the requirements. This mapping would help minimize confusion as each owner/operator's COIP and covered systems would be distinct and it may not also be practicable to draw a line exactly at a one-third assessment. The CAP must describe:

- The plan and mapping to assess the effectiveness of the owner/operator's TSA approved COIP;

- The schedule and scope of an architectural design review[193] within 12 months either before or after TSA's approval of the owner/operators COIP, to be repeated at least once

---

[190] Bureau of Transportation Statistics. (Apr. 18, 2023). "2022 Annual Average Domestic Air Fares Increases from 2021." Retrieved from: https://www.bts.gov/newsroom/2022-annual-average-domestic-air-fares-increases-2021. Accessed August 1, 2023.

[191] § 1580.329 Cybersecurity Assessment Plan, § 1582.229 Cybersecurity Assessment Plan, and § 1586.229 Cybersecurity Assessment Plan

[192] Critical Cyber Systems are defined in the definitions § 1580.313, § 1582.213, and § 1586.213 of this proposed rule text.

[193] The architectural design review 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.

every two years thereafter;

- 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, in including the use of "red" and "purple" team (adversarial perspective) testing.

The CAP must also include a schedule for conducting the assessments required. At a minimum, the schedule must ensure: compliance with biennial architecture design review and at least one-third of the policies, procedures, measures, and capabilities in the TSA-approved COIP are assessed each year resulting in 100 percent being assessed at least once over three years. In this analysis, TSA assumes one-third each year. TSA also assumes this will be done by a third party vendor.

For 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.

In addition, the owner/operator must ensure a report of the results of assessments conducted in accordance with the CAP are provided to all individuals designated under each of the covered modes 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—

- 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
- Results of the individual assessment methodologies.

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. 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.

To accomplish the above requirements, TSA estimates a range to conduct this assessment, including mapping, from 10 hours to 80 hours with a primary estimate of 40 hours. TSA assumes this would be completed by an individual with comparable responsibility of the cybersecurity analyst. Following the assessment, individuals with comparable responsibility of the network systems engineer and the COM would each spend 2 hours for a total of 4 hours each year reviewing the assessment and a total burden of 44 hours annually for CAP assessment. Within the 2 hours attributed to the COM, that individual would review the assessment as well as submit the CAP report to TSA. While TSA assumes the first mapping would be the most burdensome, it is expected that each owner/operator would be able to develop this mapping as part of their overall CAP development and assessment. TSA requests comment on this assumption.

TSA also estimates that each owner/operator would spend 40 hours every 2 years to implement the CAP and conduct the ADR and that this would also include penetration testing. While penetration testing is not a stated rule requirement, TSA is including representative costs to reflect actions that may be taken by companies as a part of their processes to be in full compliance with the provisions of the proposed rule in pursuit of a strong CRM program. Based on SME discussion, TSA estimates the potential costs of penetration testing can range widely depending on a variety of factors, including owner/operator size and systems tested. TSA uses an

average cost of $20,000 as within a range of $10,000 to $30,000.[194] As the cost involved on this task may vary greatly across owner/operators and third party providers, TSA requests comment on this estimate.

The CAP must also include a schedule to ensure completion of planned assessments. The schedule must ensure at least one-third of the policies, procedures, measures, and capabilities in the COIP are assessed each year resulting in a minimum of 100 percent assessment every three years (if an entity chose to do a 50 percent assessment in Year 1, they would still be obligated to do assessments of at least one-third of the policies, procedures, measures and capabilities of the COIP in both Year 2 and Year 3). TSA SMEs with cybersecurity expertise estimate that each owner/operator would incur a time burden of 30 hours annually to test the COIP. TSA also estimates 18 hours would be spent by a network/systems administrator with the remaining 12 hours being spent by a cybersecurity analyst. In addition to this time burden, TSA estimates that each entity would incur a flat cost of $6,667 annually, or $20,000 over three years, to enlist an outside TPV to test the COIP.[195]

TSA must also process the CAPs received. TSA anticipates it would take 32 hours to process each owner/operator CAP submitted.

2.4.8 Documentation to Establish Compliance

Each affected owner/operator would incur various recordkeeping costs.[196] This could entail

---

[194] RSI Security. What Is The Average Cost Of Penetration Testing?. May 5, 2023, available at https://blog.rsisecurity.com/what-is-the-average-cost-of-penetration-testing/. Accessed September 25, 2023.

[195] TSA estimates the three-year cost to test the COIP based on the commercial vendor sourced estimate of $20,000 to conduct penetration testing. TSA estimates the level of effort for a third party to conduct penetration testing is roughly equivalent to the effort required by an owner/operator to conduct testing of the COIP.

[196] § 1580.331 Documentation to establish compliance, § 1582.231 Documentation to establish compliance, and § 1586.231 Documentation to establish compliance

retaining documents that would be created as part of the CRM process as well as accessing and making these documents available to TSA, as requested. The costs incurred as part of the development of the CRM program are detailed in the discussion of the specific provision, as laid out in above sections. TSA estimates 2 hours of administrative assistant time in each year to meet these recordkeeping obligations. While some of the necessary compliance parameters would be covered under specific rule provisions as part of efforts to comply with the requirements of this proposed rule, TSA additionally estimates an audit manager would incur 40 hours of time to ensure overall compliance with the full rule each year.

2.4.9 Physical Security Coordinator

This provision requires covered pipeline owner/operators to provide in writing to TSA the names, titles, phone number(s), and email address(es) of the physical security coordinator and alternate physical security coordinator(s) within seven days of the commencement of new operations or change in any of the information required. The coordinator or alternate must be accessible to TSA 24 hours per day, seven days per week and serve as the primary contact for intelligence information and security-related activities and communications with TSA as well as working with appropriate law enforcement and emergency response agencies in addressing cybersecurity threats or responding to cybersecurity incidents. The coordinator(s) and alternates must be U.S. citizens eligible for a security clearance, unless otherwise waived by TSA. The cost of this requirement is the time each entity takes to designate a physical security coordinator and alternate and to submit that information to TSA. TSA estimates all covered owner/operators would provide this information in Year 1 of the proposed rule; thereafter, covered owner/operators would provide updated information to account for turnover or changes in names, titles, phone number(s), or email address(es) each year. TSA estimates a time burden of

0.5 hours of audit manager time per designated physical security coordinator.[197]

2.4.10 Reporting Physical Security Incidents

Under the proposed rule, each covered pipeline entity is required to report any potential threats and significant physical security concerns involving transportation-related operations to TSA as soon as practicable, but no later than 24 hours after an incident is identified. The reporting entity must include the contact information of the reporting individual, the affected systems, a description of the incident and threat, earliest known date of compromise, date of detection and other relevant information. TSA estimates that 25.29 calls will be made per pipeline entity per year to report such physical security incidents.[198] Based on the impacted pipeline entity population (115), this results in a total of 2,908 incidents reported each year.[199] Based on conversations with SME, TSA also estimates a time burden of 0.05 hours per call that would be performed by the physical security coordinator.[200] TSA must also receive and record this information submission. The costs to TSA are, on average, 0.32 hours per submission to receive and record this information.

2.4.11 Burden Hour Summary and Apportionment

Across each mode, TSA calculates the cost impact for each requirement using a blended or weighted average wage rate based upon the type of position likely to perform aspects or elements of the proposed rule requirements. The blended wage rates multiply the number of hours per occupation involved by the corresponding occupation wage rate for each occupation covered by

---

[197] Based on input from SMEs in the Surface Division, TSA assumes an industry manager will spend 30 minutes per submission and a TSA program analyst will spend, on average, 10 minutes per submission to record this information.

[198] This estimate is derived from a historical average based on current voluntary reporting.

[199] The total number of incidents is calculated as 25.29 calls × 115 entities = 2,908 incidents

[200] TSA data from the Transportation Security Operations Center (TSOC) shows that the average phone call is approximately 3 minutes (0.05 hours) in duration.

the requirement and divides the result by the requirement's total burden estimate. As an illustrative example, if for instance, a requirement would take 10 total hours to complete each year, and a network/systems engineer, at a wage of $50 per hour, would spend 6 hours (60%) completing the requirement and a cybersecurity analyst, at a wage of $100 per hour, would spend 4 hours (40%) the corresponding blended wage rate calculation is $70 (($50 per hour [network/systems engineer wage] × 6 hours) + ($100 per hour [cybersecurity analyst wage] × 4 hours)) ÷ 10 hours). These values represent the opportunity cost of each positions time associated with performing the activity identified. TSA does not have insight into how such activities will be distributed among new or existing staff and does not quantify new position or hiring costs but acknowledges that owner/operators may incur such costs if additional personnel are needed to comply with the requirements of the proposed rule. Table 2-10 shows the apportionment of hours, by occupation code, for each provision of the proposed rule, for industry. Similarly, Table 2-11 shows the apportionment of hours, by grade level, for each provision of the proposed rule, for TSA.

Table 2-10: Burden Hour Apportionment

Requirement	Total Hour Burden	Accountable Executive	Cybersecurity Operations Manager (COM)	Cybersecurity Coordinator	Cybersecurity Analyst	Network and Computer Systems Administrator	All Cyber Positions	Audit Manager	All Positions	Administrative Assistant	Attorney	Physical Security Coordinator
Applicability	1	0.5									0.5	
		50%									50%	
Familiarization (Freight Rail, PTPR, and Pipeline)	14.66	0.3	7.3								7.1	
		2%	50%								48%	
Familiarization (OTRB)	1	1.0										
		100%										
CSE (Freight Rail and PTPR)	40				30.0	10.0						
					75%	25%						
CSE (Pipeline)	120				60.0	60.0						
					50%	50%						
CSE Implementation	40				20.0	20.0						
					50%	50%						
COIP Review Year 1	40		20.0								20.0	
			50%								50%	
COIP Review Years 2-10	13		6.7								6.7	
			50%								50%	
Network Segmentation Year 1	820		340.0		192.0	288.0						
			41%		23%	35%						
Network Segmentation Years 2-10	660		180.0		192.0	288.0						
			27%		29%	44%						
Access Control Year 1	100		66.7		13.3	20.0						
			67%		13%	20%						
Access Control Years 2-10	58.34		25.0		13.3	20.0						
			43%		23%	34%						

Requirement	Total Hour Burden	Accountable Executive	Cybersecurity Operations Manager (COM)	Cybersecurity Coordinator	Cybersecurity Analyst	Network and Computer Systems Administrator	All Cyber Positions	Audit Manager	All Positions	Administrative Assistant	Attorney	Physical Security Coordinator
Access Control Implementation	7.17								7.2			
									100%			
Detection of Cybersecurity Incidents Year 1	106.5		12.0			94.5						
			11%			89%						
Detection of Cybersecurity Incidents Years 2-10	100.5		6.0			94.5						
			6%			94%						
Patching Year 1	82		4.0			78.0						
			5%			95%						
Patching Years 2-10	80		2.0			78.0						
			3%			98%						
Patching Implementation	1,500					1500.0						
						100%						
POAM	80				32.0	48.0						
					40%	60%						
Identification of Accountable Executive	3 hours per individual		1.0								2.0	
			33%								67%	
Cybersecurity Coordinator	2 hours per individual			0.8	0.3						1.0	
				38%	13%						50%	
Identification of Critical Cyber Systems Year 1)	160		80.0		48.0	32.0						
			50%		30%	20%						
Identification of Critical Cyber Systems Years 2-10	40		20.0		12.0	8.0						
			50%		30%	20%						
Supply Chain Risk Management	330		165.0		115.5	49.5						
			50%		35%	15%						
	12					12.0						

Requirement	Total Hour Burden	Accountable Executive	Cybersecurity Operations Manager (COM)	Cybersecurity Coordinator	Cybersecurity Analyst	Network and Computer Systems Administrator	All Cyber Positions	Audit Manager	All Positions	Administrative Assistant	Attorney	Physical Security Coordinator
Data Backup Supervision						100%						
Cybersecurity Training Plan Submissions	80		80.0									
			100%									
Basic Cybersecurity Training	1 hour per individual								1.0			
									100%			
Role-based Cybersecurity Training	2 hours per individual						2.0					
							100%					
Cybersecurity Training Recordkeeping	0.02 hours per record									0.02		
										100%		
Cybersecurity Incident Reporting	1 hour per incident		0.5		0.5							
			50%		50%							
CIRP Year 1	80		80.0									
			100%									
CIRP Years 2-10	20		20.0									
			100%									
CIRP Implementation	160				64.0	96.0						
					40%	60%						
CIRP Effectiveness Testing	120		120.0									
			100%									
CAP	44		2.0		40.0	2.0						
			5%		91%	5%						
CAP Implementation	40				16.0	24.0						
					40%	60%						
CAP Related COIP Testing	30				12.0	18.0						
					40%	60%						

Requirement	Total Hour Burden	Accountable Executive	Cybersecurity Operations Manager (COM)	Cybersecurity Coordinator	Cybersecurity Analyst	Network and Computer Systems Administrator	All Cyber Positions	Audit Manager	All Positions	Administrative Assistant	Attorney	Physical Security Coordinator
Recordkeeping	2									2.0		
										100%		
Compliance (Freight Rail, PTPR, and Pipeline)	40							40.0				
								100%				
Physical Security Coordinator	0.5 hours per individual							0.5				
								100%				
Physical Security Incident Reporting	0.05 hours per incident											0.05
												100%
Sum of Hours Per Occupation, Year 1		1.8	813.5	0.8	643.6	2,352.0	2.0	40.5	8.2	2.02	30.6	0.05
Sum of Hours Per Occupation, Annual Years 2-10		1.8	635.5	0.8	607.6	2,328.0	2.0	40.5	8.2	2.02	17.2	0.05

Note: Values rounded to hundredth decimal place unless otherwise displayed.

Table 2-11 depicts the burden hours of the proposed rule, by provision, to TSA. The tables present both the Year 1 hours as well as the expected future year incurred hours.

Table 2-11: TSA Burden Hour by Provision

Requirement	Responsible GS Equivalent	Total Hour Burden
Pipeline Physical Security Incident Report	2 x I-Band (0.16 hours) 2 x J-Band (0.16 hours)	0.32
CSE Review	2 x I-Band (2 hours) 2 x J-Band (2 hours)	4
COIP Review (Year 1)	J-Band (42 hours) K-Band (8 hours)	50
COIP Review (Years 2-10)	J-Band (14 hours) K-Band (2.67 hours)	16.67
COIP Legal Review	K-Band	4
COIP-Related Training (Years 1-3)	J-Band	160
COIP-Related Training (Years 4-10)	J-Band	40
Process Accountable Executives Information	2 x I-Band (2.5 hours) 2 x J-Band (2.5 hours)	5
Process Cybersecurity Coordinators Information	2 x I-Band (0.5 hours) 2 x J-Band (0.5 hours)	1
Process Cybersecurity Training Plans	2 x I-Band (20 hours) 2 x J-Band (20 hours)	40
Inspect Cybersecurity Training Records	H-Band	4
TSI Training	2 x I-Band (2 hours) 2 x J-Band (2 hours)	4
CIRP Review	2 x I-Band (2 hours) 2 x J-Band (2 hours)	4
Cybersecurity Incident Response (per incident)	2 x I-Band (16 hours) 2 x J-Band (16 hours)	32
CAP Review	2 x I-Band (16 hours) 2 x J-Band (16 hours)	32
Sum of Hours (Year 1)		340.3
Sum of Hours (Years 2-10)		187.0

3 COST IMPACTS TO REGULATED INDUSTRIES AND GOVERNMENT

This section details the costs associated with the implementation and operation of the proposed rule. TSA presents the costs incurred by impacted owner/operators across four modal populations including freight rail in Section 3.1, passenger rail and transit in Section 3.2, highway and motor carrier in Section 3.3, and pipeline in Section 3.4 as well as costs incurred by TSA in Section 3.5. Within each section, subsections detail the regulatory requirements for cybersecurity risk management and the associated cost components for each affected population over a ten-year period of analysis using assumptions and data from Section 2. Costs vary for the different surface modes covered by this proposed rule in accordance with inherent modal differences. Finally, Section 3.6 summarizes the total cost of the proposed rule.

3.1 Cost Impacts to Freight Railroads

This section details the costs to freight railroad owner/operators associated with the creation and maintenance of a CRM Program as detailed in the proposed rule. Section § 1580.303 of the proposed rule details the components that covered entities would be required to have in their CRM programs as well as parameters for subsidiaries. These include a cybersecurity evaluation (CSE), a TSA-approved Cybersecurity Operational Implementation Plan (COIP), and a Cybersecurity Assessment Plan (CAP) whose costs are discussed in Sections 3.1.2 (CSE), 3.1.3 (COIP), and 3.1.6 (CAP) accordingly. Additional costs related to familiarization, reporting cybersecurity incidents, and recordkeeping and documentation are also included below.

3.1.1 Familiarization Cost

TSA anticipates freight railroad owner/operators would incur a familiarization cost to review the proposed rule requirements and determine applicability. Familiarization cost includes the time it

takes to review the proposed rule's specifications and determine what is needed to achieve compliance. TSA uses a two-pronged approach to estimate familiarization cost. TSA first estimates that each owner/operator across the full industry would review the applicability portion of the rule to determine if they are covered under the scope. According to data from the Association of American Railroads, there are 620 freight railroads in the industry.[201] TSA assumes Class I freight railroads will remain static, while the remaining 614 freight railroads will experience a growth rate of 0.85 percent. TSA expects an attorney and an individual with the equivalent responsibility of the accountable executive would each spend a half hour reviewing the applicability portion of the rule for a total burden of one hour.[202] TSA next calculates a weighted average compensation rate of $166.41 per hour using the fully-loaded wage rate for an attorney of $130.21 and accountable executive of $202.60 per hour from Section 2.3.1.[203] TSA then multiplies the weighted average compensation rate ($166.41) by the applicability determination hour burden (1 hour) and number of freight railroads per year to calculate a total freight rail applicability determination cost.

TSA estimates that a COM and an attorney from each affected owner/operator would each spend an average of 7.08 hours to review the regulation, as discussed in Section 2.4.1. TSA additionally estimates that 15 minutes of time will be taken for a COM to brief an accountable executive on the requirements of the rule.

TSA next calculates a weighted average compensation rate of $129.88 per hour using the fully-

---

[201] Association of American Railroads (AAR). Jul. 2023. Freight Rail Facts & Figures. https://www.aar.org/facts-figures. Accessed on July 17, 2023.

[202] TSA estimates this as a small hour burden based upon the applicability section being short (less than one page) and the reader's inherent knowledge of their company.

[203] TSA calculates the weighted compensation rate as (($130.21 × 0.5 hours) + ($202.60 × 0.5 hours)) ÷ 1 hour. Value used in analysis is rounded to two decimal places.

loaded wage rate for a COM of $127.10, an attorney of $130.21, and accountable executive of $202.60 per hour.[204] TSA then multiplies the weighted average compensation rate by the rule review hour burden (14.66 hours) to calculate a freight rail rule review cost.

Table 3-1 presents the total freight rail familiarization cost over time. It includes applicability determination and rule review costs.

Table 3-1: Freight Rail Familiarization Cost ($ Thousands)

Year	Entire Freight Rail Population (Growth)	Applicability Determination Cost	Freight Rail Affected Population (Growth)	Rule Review Cost	Total Freight Rail Familiarization Cost
	a = 6 + (614 × (1 + 0.85%) ^ (Y_n – 1)) - ∑($a_{Yn...}$ a_{Yn} – 1)	b = a × 1 hour × $166.41	c = Column b, Table 2-1	d = c × 14.66 hours × $129.88	e = b + d
1	620.00	$103.2	73.00	$139.0	$242.2
2	5.22	$0.9	0.57	$1.1	$2.0
3	5.26	$0.9	0.57	$1.1	$2.0
4	5.31	$0.9	0.58	$1.1	$2.0
5	5.35	$0.9	0.59	$1.1	$2.0
6	5.40	$0.9	0.59	$1.1	$2.0
7	5.45	$0.9	0.59	$1.1	$2.0
8	5.49	$0.9	0.60	$1.1	$2.1
9	5.54	$0.9	0.60	$1.1	$2.1
10	5.58	$0.9	0.61	$1.2	$2.1
Total		**$111.3**		**$149.1**	**$260.3**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed. Formulas with X_{yn-1} in year one are equal to the initial value of X_{y1}.

3.1.2 Cybersecurity Evaluation (CSE) Cost

The CSE provision requires that each owner/operator required to have a CRM program complete an initial and recurrent cybersecurity evaluation. The cost of this requirement relates to the time burden for entities to conduct the evaluation as well as any costs incurred to immediately address risks identified. TSA SMEs with cybersecurity expertise first estimate an annual average time to conduct this evaluation of 40 hours, which includes 30 hours of a cybersecurity analyst time and

[204] TSA calculates the total time burden as 14.66 = (7.08 hours × 2) + 0.25 hours + 0.25 hours. TSA calculates the weighted compensation rate as (($202.60 × 0.25 hours) + ($127.10 × 7.33 hours) + ($130.21 × 7.08 hours)) ÷ 14.66 hours. Value used in analysis is rounded to two decimal places.

10 hours of a network/systems administrator's time. TSA next calculates a weighted average compensation rate of $66.66 per hour using the fully-loaded wage rate for a cybersecurity analyst of $67.34 and network/systems administrator of $64.63 per hour as discussed in Section 2.3.1. TSA then multiplies the weighted average compensation rate ($66.66) by the evaluation hour burden (40 hours) and number of freight railroads per year to calculate freight rail evaluation costs per year.

Next, TSA assumes some entities would choose to immediately plan how to address some of the risk areas discovered while others would wait to address risks through their COIP. Surface transportation SMEs estimate that 20 percent of owner/operators would begin to plan to address risks immediately upon completion of their evaluation while the remaining 80 percent would take further mitigation action as part of COIP implementation. TSA assumes that such efforts would occur each year following the evaluation and that a cybersecurity analyst and network/systems administrator would each spend an average of 20 hours planning to address identified risks for a total of 40 hours.[205] TSA next calculates a weighted average compensation rate of $65.99 per hour using the fully-loaded wage rate for a cybersecurity analyst of $67.34 and network/systems administrator wage rate of $64.63 per hour.[206] TSA then multiplies the weighted average compensation rate ($65.99) by the evaluation risk reduction hour burden (40 hours), percent of owner/operators who take action (20 percent), and number of freight railroads per year to calculate a freight rail evaluation risk reduction cost.

---

[205] TSA calculates the estimated time burden as twenty (20) hours for a cybersecurity analyst + twenty (20) hours for network/systems administrator = forty (40) hours total. TSA assumes any procurement needs, such as hardware or software, may be identified during the CSE but upgrades would happen as part of the overall COIP implementation or in the course of normal business practices.

[206] TSA calculates the weighted compensation rate as ($67.34 × 20 hours) + ($64.63 × 20 hours) ÷ 40 hours. Value used in analysis is rounded to two decimal places.

Table 3-2 presents the total freight rail CSE cost over 10 years. It includes cybersecurity evaluation and risk reduction costs.

Table 3-2: Cybersecurity Evaluation (CSE) for Freight Rail ($ Thousands)

Year	Freight Affected Rail Population	CSE Annual Evaluation Cost	Implementation Population	CSE Implementation Cost	Total CSE Cost
	a = Column a, Table 2-1	b = a × 40 hours × $66.66	c = a × 20%	d = c × 40 hours × $65.99	e = b + d
1	73.00	$194.6	14.60	$38.5	$233.2
2	73.57	$196.2	14.71	$38.8	$235.0
3	74.14	$197.7	14.83	$39.1	$236.8
4	74.72	$199.2	14.94	$39.4	$238.7
5	75.31	$200.8	15.06	$39.8	$240.6
6	75.90	$202.4	15.18	$40.1	$242.4
7	76.49	$204.0	15.30	$40.4	$244.3
8	77.09	$205.6	15.42	$40.7	$246.3
9	77.69	$207.2	15.54	$41.0	$248.2
10	78.30	$208.8	15.66	$41.3	$250.1
Total		**$2,016.4**		**$399.2**	**$2,415.6**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

3.1.3 Cybersecurity Operational Implementation Plan (COIP) Cost

Each owner/operator required to have a CRM program must adopt a Cybersecurity Operational Implementation Plan (COIP). The development and implementation of one's COIP involves a level of governance that includes identifying information about the owner/operator, including an accountable executive responsible for the sustainment of the company's cybersecurity program and providing a written attestation that the plan has been reviewed, and identification of operations which meet the applicability requirements. The COIP also requires owner/operators to address specific content, including the designation of cybersecurity coordinators, identification of Critical Cyber Systems requiring protection, and creating policies and procedures to protect Critical Cyber Systems, detect cybersecurity incidents, and to respond to detected cybersecurity incidents. The COIP also requires owner/operators to develop and implement cybersecurity training for general and IT specialist populations, develop standards for ensuring supply chain risk management, backup Critical Cyber Systems, and develop capabilities to respond to a

cybersecurity incident. Furthermore, to the extent that the owner/operator does not meet the requirements mentioned above, the owner/operator must create a plan of action and milestones (POAM) to achieve those outcomes. The costs associated with these COIP requirements are detailed in the subsections below.

3.1.3.1 Governance of the CRM Program Cost

TSA estimates owner/operators would spend 40 hours setting up an initial COIP in Year 1 and providing identifying information as discussed in Section 2.4.4. For years 2-10, TSA assumes owner/operators would spend 40 hours, in any one year in a three-year period, presented as an annual average of 13.33 hours. TSA assumes time spent on this requirement would be evenly split between a COM and a corporate attorney. TSA calculates a weighted average compensation rate of $128.66 per hour using the fully-loaded wage rate for an attorney of $130.21 and of $127.10 per hour for the COM. [207] TSA then multiplies the weighted average compensation rate ($128.66) by the COIP development hour burden (40 hours) and number of affected freight railroads per year to calculate a freight rail COIP development cost in Year 1. TSA then multiplies the weighted average compensation rate ($128.66) by the subsequent year COIP development burden (13.33 hours) and number of affected freight rail entities per year to calculate a freight rail COIP development cost in Years 2-10.

In addition, owner/operators must identify an accountable executive of the organization responsible for the sustainment of the company's cybersecurity program and have final approval authority over program parameters. The cost of this requirement is the time it takes each affected owner/operator to identify such an executive-level individual. Given the complexity of CRM

[207] TSA calculates the weighted compensation rate as ($130.21 × 20 hours) + ($127.10 × 20 hours) ÷ 40 hours. Value used in analysis is rounded to two decimal places.

programs, TSA recognizes that some entities may require more than one individual to hold this designation but for purposes of this analysis, has assumed that affected owner/operators will select one individual in order to meet the requirements of the rule, as shown in Table 3-3.

Table 3-3: Accountable Executive Population for Freight Rail

Year	Freight Rail Affected Population	Number of Initial Accountable Executives	Number of Additional Accountable Executives Resulting From Employee Turnover	Total Number of Accountable Executives
	a = Column a, Table 2-1	$b_{Y1} = a_{Y1}$ $b_{Yn} = a_{Yn} - a_{Yn-1}$	$c_{Y1} = 0$ $c_{Yn} = a \times 4\%$	d = b + c
1	73.00	73.00	0	73.00
2	73.57	0.57	2.94	3.51
3	74.14	0.57	2.97	3.54
4	74.72	0.58	2.99	3.57
5	75.31	0.59	3.01	3.60
6	75.90	0.59	3.04	3.63
7	76.49	0.59	3.06	3.65
8	77.09	0.60	3.08	3.68
9	77.69	0.60	3.11	3.71
10	78.30	0.61	3.13	3.74
Total		**78**	**27**	**106**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise shown. Formulas with X_{yn-1} in year one are equal to the initial value of X_{y1}.

TSA estimates owner/operators would spend three hours making this determination per identified individual, split between one hour of COM time to make the designation and two hours of attorney time to review and document the qualifying criteria. TSA next calculates a weighted average compensation rate of $129.17 per hour using the fully-loaded wage rate for a COM of $127.10 and attorney of $130.21 per hour.[208]

In addition, TSA estimates an accountable executives turnover rate of 4 percent, based on BLS data, that would necessitate a new designation as discussed in Section 2.2. TSA then multiplies the number of accountable executives by the hour burden per accountable executive and the

[208] TSA calculates the weighted compensation rate as ($130.21 × 2 hours) + ($127.10 × 1 hour) ÷ 3 hours. Value used in analysis is rounded to two decimal places.

weighted average compensation wage to determine the accountable executive designation cost for entities. The total accountable executive designation cost is presented in Table 3-4.

Table 3-4: COIP Governance Cost for Freight Rail ($ Thousands)

Year	New Freight Rail Entities	Existing Freight Rail Population	COIP Development	Freight Rail Accountable Executive Population	Accountable Executive Designation Cost	Freight Rail Total COIP Governance Cost
	a = Column b, Table 2-1	$b_{y1} = 0$ $b_{Yn} = a_{Yn-1} + b_{Yn-1}$	c = (a × 40 hours × $128.66) + (b × 13.33 hours × $128.66)	d = Column a, Table 3-3	e = d × 3 hours × $129.17	f = c + e
1	73.00	0.00	$375.7	73.00	$28.3	$404.0
2	0.57	73.00	$128.1	3.51	$1.4	$129.5
3	0.57	73.57	$129.1	3.55	$1.4	$130.5
4	0.58	74.14	$130.1	3.57	$1.4	$131.5
5	0.59	74.72	$131.2	3.61	$1.4	$132.6
6	0.59	75.31	$132.2	3.64	$1.4	$133.6
7	0.59	75.90	$133.2	3.65	$1.4	$134.6
8	0.60	76.49	$134.3	3.69	$1.4	$135.7
9	0.60	77.09	$135.3	3.71	$1.4	$136.7
10	0.61	77.69	$136.4	3.74	$1.4	$137.8
Total			**$1,565.6**		**$40.9**	**$1,606.6**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed. Formulas with X_{yn-1} in year one are equal to the initial value of X_{y1}.

3.1.3.2 Cybersecurity Coordinator Cost

This provision requires owner/operators to provide in writing to TSA the names, titles, phone number(s), and email address(es) of the cybersecurity coordinator and alternate cybersecurity coordinator(s) within seven days of the commencement of new operations or change in any of the information required by this section. The cost of this requirement is the time each entity takes to designate a cybersecurity coordinator and alternate and to submit that information to TSA. TSA estimates all covered owner/operators would provide this information in Year 1 of the proposed rule; thereafter, covered owner/operators will need to provide updated information to account for turnover or changes in names, titles, phone number(s), or email address(es) each year. TSA estimates a 4 percent turnover rate as discussed in Section 2.2.

Each owner/operator vets the qualifications of the cybersecurity coordinator to determine if they

meet the requirements of the role. TSA estimates that all entities would have two individuals filling this role of coordinator and alternate. TSA estimates that a COM will take 15 minutes of time to designate the cybersecurity coordinator, each designated cybersecurity coordinator would take 45 minutes of their time to provide contact details to TSA, and an attorney would spend one hour of time to review, select, and vet the identified individual to ensure the qualifications of the designated individuals. This results in a total of two hours per designation. TSA next calculates a weighted average compensation rate of $128.66 per hour using the fully-loaded wage rate for a cybersecurity coordinator of $127.10, for a COM of $127.10 and for an attorney of $130.21.[209] TSA then multiplies the number of designated cybersecurity coordinators by the hour burden per coordinator and the weighted average compensation wage ($128.66) to determine the cybersecurity coordinator designation cost for covered entities as presented in Table 3-5.

[209] TSA calculates the weighted compensation rate as ($130.21 × 1 hour) + ($127.10 × 0.25 hour) + ($127.10 x 0.75 hours) ÷ 2 hours. Value used in analysis is rounded to two decimal places.

Table 3-5: Cybersecurity Coordinator Cost for Freight Rail ($ Thousands)

Year	Freight Rail Affected Population	Number of Cybersecurity Coordinators	Number of Additional Cybersecurity Coordinators Resulting From Employee Turnover	Total Number of Cybersecurity Coordinators	Freight Rail Cybersecurity Coordinator Cost
	a = Column a, Table 2-1	$b_{y1} = a_{y1} \times 2$ $b_{yn} = (a_{yn} - a_{yn-1}) \times 2$	$c_{y1} = 0$ $c_{yn} = a_{yn} \times 2 \times 4.00\%$	d = b + c	e = d × 2 hours × $128.66
1	73.00	146.00	0	146.00	$37.6
2	73.57	1.14	5.89	7.03	$1.8
3	74.14	1.14	5.93	7.07	$1.8
4	74.72	1.16	5.98	7.14	$1.8
5	75.31	1.18	6.02	7.20	$1.9
6	75.90	1.18	6.07	7.25	$1.9
7	76.49	1.18	6.12	7.30	$1.9
8	77.09	1.20	6.17	7.37	$1.9
9	77.69	1.20	6.22	7.42	$1.9
10	78.30	1.22	6.26	7.48	$1.9
Total		**157**	**55**	**211**	**$54.4**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed. Formulas with X_{yn-1} in year one are equal to the initial value of X_{y1}.

3.1.3.3 Identification of Critical Cyber Systems Costs

Under the proposed rule, owner/operators must incorporate a list of Critical Cyber Systems, as defined in the TSA Cybersecurity Lexicon, into its COIP that provides at a minimum an identifier and system specific information, such as the system/manufacturer/designer name for each Critical Cyber System. The owner/operator must also discuss its identification methodology and provide system architecture and connection information. Affected owner/operators would incur costs to design its identification protocol and conduct a review of its inventory to designate Critical Cyber Systems, and ensure such systems are defined in the TSA Cybersecurity Lexicon.[210] TSA estimates affected entities would spend an average of 160 hours in Year 1 performing these tasks and 40 hours in subsequent years (Years 2 through 10) to review and

[210] See Section III(F)(2) of the Notice of Proposed Rulemaking for information on TSA's Cybersecurity Lexicon.

update.[211] In Year 1, these 160 hours are associated with designing the criteria, conducting an IT and OT inventory, creating a database, keeping it up to date, and integrating criticality designations. For Years 2 through 10, TSA estimates there will be some efficiency gains from experience implementing these processes. TSA assumes these tasks would be performed by the COM, network/systems administrator, and a cybersecurity analyst as shown in Table 2-10.

TSA calculates a weighted average compensation rate of $96.68 per hour using the fully-loaded wage rate for a cybersecurity analyst of $67.34 for a network/systems administrator of $64.63, and for a COM of $127.10 per hour.[212]

TSA uses the same wage rate for Year 1 multiplied by the new entity hour burden to identify Critical Cyber Systems (160 hours) plus the wage rate for existing entities multiplied by the existing entity hour burden (40 hours) to calculate a Critical Cyber Systems identification cost as presented in Table 3-6 below.

[211] TSA SMEs with cybersecurity expertise estimate an hour burden range of 80 – 244 hours for Year 1 and a range of 40 – 120 hours for Years 2-10. TSA uses an hour burden of 160 hours for Year 1 as it assumes most entities would be near the middle of the range in Year 1 and 40 hours for Years 2-10 as it believes efficiencies in processes would provide an average cost closer to the low end of the range.

[212] TSA calculates the weighted compensation rate as ($127.51 × 160 hours × 50%) + ($67.56 × 160 hours × 30%) + ($64.84 × 160 hours × 20%). Value used in analysis is rounded to two decimal places.

Table 3-6: Identification of Critical Cyber Systems Costs for Freight Rail ($ Thousands)

Year	New Freight Rail Affected Entities	Existing Freight Rail Affected Population	New Entity Critical Cyber System Cost	Existing Entity Critical Cyber System Cost	Total Freight Rail Identification of Critical Cyber Systems Cost
	a = Column b, Table 2-1	$b_{y1} = 0$ $b_{Yn} = a_{Yn-1} + b_{Yn-1}$	c = a × 160 hours × $96.68	d = b × 40 hours × $96.68	e = c + d
1	73.00	0.00	$1,129.2	$0.0	$1,129.2
2	0.57	73.00	$8.8	$282.3	$291.1
3	0.57	73.57	$8.8	$284.5	$293.3
4	0.58	74.14	$9.0	$286.7	$295.7
5	0.59	74.72	$9.1	$289.0	$298.1
6	0.59	75.31	$9.1	$291.2	$300.4
7	0.59	75.90	$9.1	$293.5	$302.6
8	0.60	76.49	$9.3	$295.8	$305.1
9	0.60	77.09	$9.3	$298.1	$307.4
10	0.61	77.69	$9.4	$300.4	$309.9
Total			**$1,211.2**	**$2,621.6**	**$3,832.8**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed. Formulas with X_{yn-1} in year one are equal to the initial value of X_{y1}.

3.1.3.4 Supply Chain Risk Management Costs

Under the proposed rule, owner/operators must incorporate into their COIP policies, procedures, and capabilities to address supply chain cybersecurity vulnerabilities. This includes ensuring all procurement documents and contracts include a requirement for the vendor or service provider to notify the owner/operator of cybersecurity incidents, vulnerabilities, and an evaluation of the cybersecurity measures implemented by vendors. In addition, owner/operators must consider the level of cybersecurity sufficient to protect against or respond to cybersecurity incidents and mitigation measures to address risks identified by the vendor or service provider. The cost of this requirement includes the time incurred for contract renewals and updates to come into compliance, as well as the time owner/operators spend to check the goods, services, or capabilities provided by vendors or service providers to identify potential vulnerabilities. TSA estimates affected entities would spend an average of 330 hours annually to perform these tasks. This includes 10 hours of attorney time to review and update contracts and 40 hours for a team of

four individuals to check vendor provided capabilities twice a year.[213] A TSA SME with cybersecurity expertise estimates checking vendor-provided capabilities would be split between a COM who will incur a time burden of 160 hours, a cybersecurity analyst who will incur 112 hours of time, and a network/systems administrator who will incur 48 hours of time.

TSA calculates a weighted average compensation rate of $97.83 per hour using the fully-loaded wage rate for an attorney of $130.21, a COM of $127.10, a cybersecurity analyst of $67.34, and for a network/systems administrator of $64.63 per hour.[214] TSA then multiplies the weighted average compensation rate ($97.83) by the supply chain risk management hour burden (330 hours) and number of freight railroads per year to calculate a freight rail supply chain risk management cost per year as presented in Table 3-7.

Table 3-7: Supply Chain Risk Management Cost for Freight Rail ($ Thousands)

Year	Freight Rail Affected Population	Supply Chain Risk Management Cost
	a = Column a, Table 2-1	b = a × 330 hours × $97.83
1	73.00	$2,356.7
2	73.57	$2,375.1
3	74.14	$2,393.5
4	74.72	$2,412.3
5	75.31	$2,431.3
6	75.90	$2,450.3
7	76.49	$2,469.4
8	77.09	$2,488.8
9	77.69	$2,508.1
10	78.30	$2,527.8
Total		**$24,413.4**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

3.1.3.5 Protection of Critical Cyber Systems Cost

Under the proposed rule, owner/operators must incorporate into its COIP network segmentation

[213] TSA estimates four (4) cybersecurity analysts would spend 40 hours twice a year. 4 analysts × 40 hours × 2 times a year = 320. 320 hours for the cybersecurity analysts + 10 hours for an attorney = 330 hours.

[214] TSA calculates the weighted compensation rate as ($130.21 × 10 hours) + ($127.10 × 160 hours) + ($67.34 × 112 hours) + ($64.63 × 48 hours) ÷ 330 hours. Value used in analysis is rounded to two decimal places.

and other policies, procedures, controls, and capabilities to protect Critical Cyber Systems that are sufficient to protect against disruption of IT and OT, secure and defend zone boundaries, control access to Critical Cyber Systems to prevent unauthorized access, reduce the risk of exploitation of unpatched systems through the application of security patches and updates, ensure logging data are stored and maintained properly, ensure all Critical Cyber Systems are regularly backed up, and other policies.

The cost related to network segmentation involves developing and implementing policies to properly segment OT and IT. TSA estimates affected entities would spend 820 hours in Year 1 and 660 hours in subsequent years (Years 2 through 10) performing this task.[215] TSA estimates the 820-hour total time burden in Year 1 is comprised of 100 hours to design the criteria, 120 hours to conduct an inventory of OT, 120 hours to review OT to OT connections, 120 hours to review OT to IT connections, 120 hours to review OT connections to third-parties, and 240 hours to develop networking solutions to ensure OT and IT are separate.

For Years 2 through 10, TSA estimates each of the above tasks would continue each year. TSA estimates the components of the time burden relating to application would remain constant and the time burden to design segmentation criteria would fall by 40 percent to 60 hours per entity per year and the time burden to design networking solutions separating IT and OT would fall by half to 120 hours per entity per year, for a total annual time burden per entity of 660 hours. TSA assumes the equivalent of a COM would perform the design component tasks, while a

[215] TSA SMEs with cybersecurity expertise estimate an hour burden range of 320 – 840 hours for Year 1 and a range of 240 – 660 hours for Years 2-10. TSA uses an hour burden of 820 hours for Year 1 and 660 hours for Years 2-10 as it believes the higher estimate better reflects the average time it would take for affected owner/operators to complete these tasks.

system/network administrator and cybersecurity analyst would perform the application component of the requirements.

TSA calculates a weighted average compensation rate of $91.17 in Year 1 using a fully-loaded wage rate for a cybersecurity analyst of $67.34, for a network/system administrator of $64.63, and for a COM of $127.10 per hour.[216] In Years 2 through 10 TSA calculates a weighted average compensation rate of $82.46 due to the lower proportion of the time burden taken up by the COM.[217]

TSA multiplies the wage rate calculated for Year 1 by the new entity network segmentation hour burden (820 hours) and adds to it the product of the Year 2 wage rate and the existing entity network segmentation hour burden (660 hours) to calculate a network segmentation cost displayed in Table 3-8 below.

[216] TSA calculates the weighted compensation rate as ($127.10 × 340 hours) + ($67.34 × 192 hours) + ($64.63 × 288 hours) ÷ 820 hours. Value used in analysis is rounded to two decimal places.
[217] TSA calculates the weighted compensation rate as ($127.10 × 180 hours) + ($67.34 × 192 hours) + ($64.63 × 288 hours) ÷ 660 hours. Value used in analysis is rounded to two decimal places.

Table 3-8: Network Segmentation Cost for Freight Rail ($ Thousands)

Year	New Freight Rail Affected Entities	Existing Freight Rail Affected Population	New Entity Cost	Existing Entity Cost	Total Freight Rail Network Segmentation Cost
	a = Column b, Table 2-1	$b_{y1} = 0$ $b_{Yn} = a_{Yn-1} + b_{Yn-1}$	c = a × 820 hours × $91.17	d = b × 660 hours × $82.46	e = c + d
1	73.00	0	$5,457.4	$0.0	$5,457.4
2	0.57	73.00	$42.6	$3,972.9	$4,015.5
3	0.57	73.57	$42.6	$4,003.9	$4,046.6
4	0.58	74.14	$43.4	$4,035.0	$4,078.3
5	0.59	74.72	$44.1	$4,066.5	$4,110.6
6	0.59	75.31	$44.1	$4,098.6	$4,142.7
7	0.59	75.90	$44.1	$4,130.8	$4,174.9
8	0.60	76.49	$44.9	$4,162.9	$4,207.7
9	0.60	77.09	$44.9	$4,195.5	$4,240.4
10	0.61	77.69	$45.6	$4,228.2	$4,273.8
Total			**$5,853.7**	**$36,894.3**	**$42,748.0**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed. Formulas with X_{yn-1} in year one are equal to the initial value of X_{y1}.

The costs related to access control involve designing and reviewing necessary criteria and solutions. TSA estimates owner/operators would spend 100 hours in Year 1 and 58.34 hours in subsequent years (Years 2 through 10) performing this task.[218] The time burden in Year 1 is comprised of 50 hours to design the criteria, 33 hours to conduct an access review, and 17 hours to design network solutions per entity. In Years 2 through 10, TSA SMEs with cybersecurity expertise estimate the 33 hours needed for access review continues unchanged, while the ongoing time burden for designing the criteria and designing the network solutions falls to 17 and 8 hours, respectively. TSA assumes these tasks would be performed by a network/systems administrator, cybersecurity analyst, and the COM.

TSA calculates a weighted average compensation rate of $106.64 per hour using a fully-loaded

[218] TSA SMEs with cybersecurity expertise estimate an hour burden range of 75 – 200 hours for Year 1 and a range of 33 - 68 hours for Years 2-10 due to the decrease in time associated with designing criteria and designing networking solutions. TSA uses an hour burden of 100 hours for Year 1 and 58.34 hours for Years 2-10 to reflect entities having hour burdens throughout the range.

wage rate for a cybersecurity analyst of $67.34, for a network/systems administrator of $64.63, and for a COM of $127.10 per hour.[219] In Years 2 through 10 TSA calculates a weighted average compensation rate of $92.03 per hour due to the lower proportion of the time burden taken up by the COM.[220]

TSA multiplies the wage rate calculated for Year 1 by the new entity access control hour burden (100 hours) and adds to it the product of the Year 2 wage rate and the existing entity access control hour burden (58.34 hours) to calculate an access control cost displayed in Table 3-9 below.

Table 3-9: Access Control Compliance Cost for Freight Rail ($ Thousand)

Year	New Freight Rail Affected Entities	Existing Freight Rail Affected Population	New Entity Access Control Cost	Existing Entity Access Control Cost	Total Freight Rail Access Control Cost
	a = Column b, Table 2-1	$b_{y1} = 0$ $b_{Yn} = a_{Yn-1} + b_{Yn-1}$	c = a × 100 hours × $106.64	d = b × 58.34 hours × $92.03	e = c + d
1	73.00	0	$778.5	$0.0	$778.5
2	0.57	73.00	$6.1	$391.9	$398.0
3	0.57	73.57	$6.1	$395.0	$401.1
4	0.58	74.14	$6.2	$398.1	$404.2
5	0.59	74.72	$6.3	$401.2	$407.5
6	0.59	75.31	$6.3	$404.3	$410.6
7	0.59	75.90	$6.3	$407.5	$413.8
8	0.60	76.49	$6.4	$410.7	$417.1
9	0.60	77.09	$6.4	$413.9	$420.3
10	0.61	77.69	$6.5	$417.1	$423.6
Total			**$835.0**	**$3,639.7**	**$4,474.7**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed. Formulas with X_{yn-1} in year one are equal to the initial value of X_{y1}.

As part of their plan to control access to Critical Cyber Systems and prevent unauthorized access, TSA estimates owner/operators would procure multi-factor authentication (MFA) software at a

[219] TSA calculates the weighted compensation rate as ($127.10 × 67 hours) + ($67.34 × 19.8 hours) + ($64.63 × 13.2 hours) ÷ 100 hours. Value used in analysis is rounded to two decimal places.

[220] TSA calculates the weighted compensation rate as ($127.10 × 25 hours) + ($67.34 × 19.8 hours) + ($64.63 × 13.2 hours) ÷ 58 hours. Value used in analysis is rounded to two decimal places.

cost of $72 per employee as discussed in Section 2.4.4.5. TSA estimates owner/operators would have to acquire access control equipment and apply it to the user accounts of all their employees. TSA multiplies the cost of MFA acquisition by the employee population for Freight Rail identified in Section 2.1.1 to obtain an MFA equipment acquisition cost.

TSA also estimates each employee would incur a time burden each time the employee uses MFA and may incur additional time burdens to manage any lockouts or password resets needed. TSA estimates each employee incurs a one minute per day time burden to use MFA for a total of 4.17 hours per year, per employee.[221] TSA assumes employees would use MFA daily to log into IT network systems such as email, chat communications, file share servers, or HR systems. Since these are systems employees engage with regularly, TSA estimates that account lockouts would be rare. TSA estimates each employee incurs a 15-minute time burden to resolve lockouts for each occurrence and estimates each employee may experience a lockout out twice every two months, for a total of 3 hours per year, per employee as discussed in Section 2.4.4.5 Together, TSA calculates each employee incurs a time burden of 7.17 hours per year per employee due to MFA requirements. TSA estimates the cost of MFA to entities using the fully-loaded mean wage rate of $53.19 for the freight employee population from Section 2.3.1. TSA multiplies the same wage rate by the employee MFA time burden (7.17 hours) to calculate an employee MFA engagement cost as shown in Table 3-10 below.

[221] TSA estimates 1 min per day per employee to access MFA for a total hour burden of 4.17 hours per year, per employee. (1 ÷ 60) × 250 working days per year = 4.17 hours.

Table 3-10: Access Control Implementation Cost for Freight Rail ($ Thousands)

Year	Freight Rail Employee Population Plus Growth	MFA Equipment Cost	MFA Implementation Cost	Total MFA Cost
	a = Column a, Table 2-2	b = a × $72	c = a × 7.17 hours × $53.19	d = b + c
1	116,960.00	$8,421.1	$44,605.3	$53,026.4
2	117,451.23	$8,456.5	$44,792.6	$53,249.1
3	117,944.53	$8,492.0	$44,980.8	$53,472.8
4	118,439.89	$8,527.7	$45,169.7	$53,697.4
5	118,937.34	$8,563.5	$45,359.4	$53,922.9
6	119,436.88	$8,599.5	$45,549.9	$54,149.4
7	119,938.51	$8,635.6	$45,741.2	$54,376.8
8	120,442.26	$8,671.8	$45,933.3	$54,605.2
9	120,948.11	$8,708.3	$46,126.3	$54,834.5
10	121,456.09	$8,744.8	$46,320.0	$55,064.8
Total		**$85,820.7**	**$454,578.6**	**$540,399.3**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

As part of their COIP, each owner/operator must develop a patch management strategy that ensures all critical security patches and updates for operating systems, applications, drivers and firmware are current. TSA estimates affected entities would spend 82 hours in Year 1 and 80 hours in Years 2 through 10 performing this task as discussed in Section 2.4.4.5. TSA estimates this time burden is comprised of four hours in Year 1 and two hours in subsequent years to create and maintain a patch strategy and 78 hours per entity per year to manage new patches. [222] TSA assumes this task would be performed by the equivalent of a system/network administrator and the COM.

TSA calculates a weighted average compensation rate of $67.68 in Year 1 using a fully-loaded wage rate for a network/system administrator of $64.63 and for a COM of $127.10 per hour.[223] In Years 2 through 10 TSA calculates a weighted average compensation rate of $66.19 per hour,

[222] TSA estimates each owner/operator would spend approximately 1.5 hours per week checking CISA's list of known vulnerabilities.

[223] TSA calculates the weighted compensation rate as ($127.10 × 4 hours) + ($64.63 × 78 hours) ÷ 82 hours. Value used in analysis is rounded to two decimal places.

due to the lower proportion of the time burden taken up by the COM.[224]

TSA multiplies the wage rate for Year 1 by the new entity patch implementation hour burden (82 hours) to yield a patch implementation cost. It then adds to it the product of the wage rate for existing entities in Years 2 – 10 and the existing entity patch implementation hour burden (80 hours) to calculate a total patch implementation cost shown in Table 3-11 below.

TSA also estimates additional owner/operator time burden due to responding to new patches. TSA estimates that each entity would need to apply patches in at least one cycle per quarter and that each entity would incur a time burden of 375 hours to complete each cycle as discussed in Section 2.4.4.5. TSA assumes this task would be performed by a system/network administrator using a fully-loaded wage rate of $64.63 per hour.

Table 3-11 presents the total freight rail patching cost over 10 years. It includes new entity patching, existing entity patching, and cost to respond to new patches.

[224] TSA calculates the weighted compensation rate as ($127.10 × 2 hours) + ($64.63 × 78 hours) ÷ 80 hours. Value used in analysis is rounded to two decimal places.

Table 3-11: Cost to Implement Patching for Freight Rail ($ Thousands)

Year	New Freight Rail Affected Entities	Existing Freight Rail Affected Population	New Entity Patching Cost	Existing Entity Patching Cost	Cost to Respond to New Patches	Total Freight Rail Patching Cost
	a = Column b, Table 2-1	$b_{Y1} = 0$ $b_{Yn} = a_{Yn-1} + b_{Yn-1}$	c = a × 82 hours × $67.68	d = b × 80 hours × $66.19	e = (a + b) × 4 cycles × 375 hours × $64.63	f = c + d + e
1	73.00	0	$405.1	$0.0	$7,077.0	$7,482.1
2	0.57	73.00	$3.2	$386.5	$7,132.2	$7,522.0
3	0.57	73.57	$3.2	$389.6	$7,187.5	$7,580.2
4	0.58	74.14	$3.2	$392.6	$7,243.7	$7,639.5
5	0.59	74.72	$3.3	$395.7	$7,300.9	$7,699.9
6	0.59	75.31	$3.3	$398.8	$7,358.1	$7,760.2
7	0.59	75.90	$3.3	$401.9	$7,415.3	$7,820.5
8	0.60	76.49	$3.3	$405.0	$7,473.5	$7,881.8
9	0.60	77.09	$3.3	$408.2	$7,531.7	$7,943.2
10	0.61	77.69	$3.4	$411.4	$7,590.8	$8,005.6
Total			**$434.5**	**$3,589.7**	**$73,310.8**	**$77,335.0**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed. Formulas with X_{yn-1} in year one are equal to the initial value of X_{y1}.

Finally, TSA estimates the cost of data backups for Critical Cyber Systems to include the cost to acquire necessary storage space for all Critical Cyber System data backed up and the time burden to supervise the backup process. TSA SMEs with cybersecurity expertise estimate an average Critical Cyber System data volume per entity in Year 1 of 500 terabytes (TB) of data.[225] TSA estimates the storage cost per TB of data backed up as $329.16 per TB per year.[226] TSA assumes entities will use a cloud-based provider to store Critical Cyber System backup data. TSA is aware that alternatives exist for affected entities and that owner/operators may not choose to store their Critical Cyber System backup data in a cloud environment. TSA invites public

[225] TSA assumes affected entities will purchase cloud-based storage sufficient to meet their Critical Cyber System data backup needs in advance at the beginning of each year. TSA request comment on the amount of storage space owner/operators will need.

[226] "Cloud Storage Pricing in 2023: Everything You Need to Know." Anina Ot. Accessed September 26, 2023. https://www.enterprisestorageforum.com/cloud/cloud-storage-pricing/. TSA uses the above article's "Cloud Storage Pricing Chart" to compare five of the six (U.S.-based) cloud storage providers. The table's final row provides a per month per TB cost estimator. The article's five point estimates average to $27.43 per TB per month (($34.67 + $24.90 + $24.08 + $26.40 + $27.00) ÷ 5). TSA multiplies the per month amount by 12 months to yield an annual cost of $329.16 per TB per year.

comment on these cost assumptions. TSA further estimates that the volume of Critical Cyber System data held by freight rail entities would grow in Years 2 through 10. TSA calculates a compound annual growth rate of Critical Cyber System data volume of 2.3 percent per year between Years 2 through 10.[227] Once the backup is complete, the data will need to be safely stored. TSA cybersecurity SMEs estimate that each backup would need to be stored for a period of one year. TSA scales the per TB per month cost above appropriately.[228]

TSA also estimates the cost associated with the time burden on freight rail entities to supervise the backup of their data. TSA SMEs with cybersecurity expertise estimate that each entity would require 12 hours per year (one hour per month) to supervise the backup of their Critical Cyber System data. TSA calculates a fully loaded wage for a network/systems administrator of $64.63 per hour to supervise the backup of Critical Cyber System data. TSA multiplies the network/systems administrator wage rate by the backup supervision hour burden (12 hours) to yield a data backup supervision cost.

Table 3-12 presents freight rail critical system backup costs over time. It includes cost of data storage and time for backup supervision.

---

[227] Alex Woodie. "Big Growth Forecasted for Big Data." https://www.datanami.com/2022/01/11/big-growth-forecasted-for-big data/#:~:text=From%202020%20to%202025%2C%20IDC,of%20data%20creation%20by%202025. Accessed July 3, 2023. TSA extracted a forecast that raw data creation is expected to grow at a compound annual rate of 23% per year per entity between 2020 and 2025. However, the author also notes that organizations only save into long-term storage roughly 10% of the data which they create each year. Therefore, the net compound annual growth rate applicable to data storage needs is 23% × 10% = 2.3% per year. TSA understands this average may not capture the exact circumstances for all industries. TSA invites public comment on this input.

[228] "Cloud Storage Pricing in 2023: Everything You Need to Know." Anina Ot. Accessed September 26, 2023. https://www.enterprisestorageforum.com/cloud/cloud-storage-pricing/.

Table 3-12: Critical System Data Backups Costs for Freight Rail ($ Thousands)

Year	Freight Rail Population	Critical System Data Size Per Entity (Terabytes)	Cost of Data Backups	Cost of Data Backup Supervision	Total Cost of Freight Rail Critical System Data Backups
	a = Column a, Table 2-1	b_{y1} = 500 $b_{yn} = b_{yn-1} \times (1 + 2.30\%)$	c = a × b × $329.16	d = a × 12 hours × $64.63	e = c + d
1	73.00	500.00	$12,014.3	$56.6	$12,071.0
2	73.57	511.50	$12,386.6	$57.1	$12,443.7
3	74.14	523.26	$12,769.6	$57.5	$12,827.1
4	74.72	535.29	$13,165.4	$57.9	$13,223.3
5	75.31	547.60	$13,574.5	$58.4	$13,632.9
6	75.90	560.19	$13,995.4	$58.9	$14,054.2
7	76.49	573.07	$14,428.4	$59.3	$14,487.8
8	77.09	586.25	$14,876.1	$59.8	$14,935.8
9	77.69	599.73	$15,336.6	$60.3	$15,396.8
10	78.30	613.52	$15,812.4	$60.7	$15,873.1
Total			**$138,359.2**	**$586.5**	**$138,945.7**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed. Formulas with X_{yn-1} in year one are equal to the initial value of X_{y1}.

3.1.3.6 Training Cost

This provision requires owner/operators to provide all employees and contractors with access to the owner/operator's IT or OT systems basic cybersecurity training that includes cybersecurity awareness to address cyber-hygiene best practices, acceptable use, risks associated with their level of privileged access, and awareness of security risks associated with their actions. The owner/operator must also provide additional role-based training to cybersecurity-sensitive employees. The cost of this provision relates to four areas, including each entity's time burden to develop and implement its cybersecurity training plans, time burdens to all employees to take basic user training, time burdens to privileged users to take role-based training, and recordkeeping.

Each owner/operator must develop, submit, and implement their cybersecurity training plans. TSA estimates freight rail entities would spend 80 hours in Year 1 to develop and implement

their cybersecurity training plans.[229] TSA estimates that this task would be performed by a Freight Rail COM using a fully-loaded wage rate of $127.10 per hour.

TSA multiplies the same wage rate by the submission hour burden (80 hours) and the entity population to generate a cybersecurity training plan development cost as shown in Table 3-13 below.

Table 3-13: Cybersecurity Training Plan Costs - Freight Rail ($ Thousands)

Year	Freight Rail Initial Submissions	Training Plan Submissions Cost
	a = Column b, Table 2-1	b = a × 80 hours × $127.10
1	73.00	$742.3
2	0.57	$5.8
3	0.57	$5.8
4	0.58	$5.9
5	0.59	$6.0
6	0.59	$6.0
7	0.59	$6.0
8	0.60	$6.1
9	0.60	$6.1
10	0.61	$6.2
Total		**$796.2**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

Basic User Awareness Training is intended to provide effective cybersecurity awareness training that helps employees understand proper cyber-hygiene and the security risks associated with their actions. A TSA SME with cybersecurity expertise estimates each employee would spend one hour per year completing this training. TSA estimates that 100 percent of the affected freight rail employee population will require basic user training, while 15 percent will require role-based training. TSA calculates basic user awareness training by multiplying the freight rail employee population, by the one hour training burden, and the fully-loaded general freight rail wage rate of $53.19 per hour as described in Section 2.3.1.

[229] See "Security Training Programs for Surface Transportation Employees – Final Rulemaking." RIN: 1652-AA55. Regulatory Impact Analysis. Page 57. TSA expects the burden hours for the initial submission of the Cybersecurity training plan to be comparable to the burden hours from the Physical Security rulemaking due to the similar length and breadth of requirements, as well as that entities may not yet have experience producing such plans.

Role-based training would consider the role of the privileged user in a cyber-incident as such users bring a unique level of risk to an organization. A privileged user is one that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform. TSA SMEs with cybersecurity expertise estimate estimates the privileged user population as 15 percent of the general user population.

TSA SMEs with cybersecurity expertise estimate privileged users would spend two hours per year completing this training. TSA calculates role-based training costs by multiplying the freight rail privileged user population, by the two hour training burden, and the fully-loaded freight rail privileged user wage rate of $97.28 per hour described in Section 2.3.1.

Finally, each owner/operator would be required to retain records of initial and recurrent cybersecurity training for everyone required to receive such training. TSA estimates owner/operators would spend 0.02 hours per record handling records for both basic user awareness training records and role-based training records.[230] TSA calculates training recordkeeping costs by multiplying the number of trainings per year by the 0.02 hour training recordkeeping burden, and the fully loaded administrative assistant's wage rate of $40.42 per hour described in Section 2.3.1.

Table 3-14 presents cybersecurity training costs for freight rail over 10 years. It includes general training, role-based training, and recordkeeping costs.

[230] TSA assumes an administrative assistant for each owner/operator would file a record of each employee's training session. TSA estimates a duration of one-minute (~0.02 hours) for an administrative staff person to file a training record.

Table 3-14: Cybersecurity Training Costs for Freight Rail ($ Thousands)

Year	Freight Rail Affected Training Population	Basic User Training Cost	Role-Based Training Cost	Training Recordkeeping Cost	Total Cybersecurity Training Cost
	a = Column a, Table 2-2	b = a × 1 hour × $53.19	c = a_{Yn} × 15% × 2 hours × $97.28	d = (a + (a × 15%)) × 0.02 hours × $40.42	e = b + c + d
1	116,960.00	$6,221.1	$3,413.4	$108.7	$9,743.2
2	117,451.23	$6,247.2	$3,427.7	$109.2	$9,784.1
3	117,944.53	$6,273.5	$3,442.1	$109.6	$9,825.2
4	118,439.89	$6,299.8	$3,456.5	$110.1	$9,866.5
5	118,937.34	$6,326.3	$3,471.1	$110.6	$9,907.9
6	119,436.88	$6,352.8	$3,485.6	$111.0	$9,949.5
7	119,938.51	$6,379.5	$3,500.3	$111.5	$9,991.3
8	120,442.26	$6,406.3	$3,515.0	$112.0	$10,033.3
9	120,948.11	$6,433.2	$3,529.8	$112.4	$10,075.4
10	121,456.09	$6,460.2	$3,544.6	$112.9	$10,117.7
Total		**$63,400.1**	**$34,786.0**	**$1,108.1**	**$99,294.2**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

3.1.3.7 Detection of Cybersecurity Incidents Cost

Under the proposed rule, owner/operators must incorporate into their COIP policies, procedures, and capabilities sufficient to detect and respond to cybersecurity threats and anomalies on Critical Cyber Systems. These policies, procedures, and capabilities must defend against malicious email, block ingress and egress communications, control the impact of known or suspected malicious web domains or applications, block and defend against unauthorized code or malicious command and control servers, and ensure continuous collection and analysis of data for potential intrusions and anomalous behavior. TSA estimates each affected entity would spend 106.5 hours in Year 1 and 100.5 hours in Years 2 through 10 performing these tasks.[231] In Year 1, this includes four hours to design continuous monitoring criteria, eight hours to develop solutions for IT, two hours per quarter for four network/systems administrators to meet to review

[231] TSA SMEs with cybersecurity expertise estimate an hour burden range of 106.5 – 211 hours for Year 1 and a range of 100.5 – 197 hours for Years 2-10. TSA uses the lower range estimates as it believes average costs would be closer to the lower values.

security threats (a total of 32 hours per year), and 15 minutes per work day for updates to the list of blocked websites (a total of 62.5 hours per year).[232] For Years 2 through 10, TSA estimates there will be efficiency gains from experience implementing these process. In Years 2 through 10 TSA estimates each affected entity would spend two hours to design the criteria, four hours to develop solutions for IT, and the continuation of the quarterly meetings and daily updates for an annual burden of 100.50 hours. TSA assumes these tasks would be performed by the COM and network/systems administrator.

TSA calculates a weighted average compensation rate of $71.67 per hour in Year 1 using the fully-loaded wage rate for a COM of $127.10 and for a network/systems administrator of $64.63 per hour. [233] TSA calculates a weighted average compensation rate of $68.36 in Years 2 through 10 due to lower participation of the COM in the time burden.[234] TSA also estimates an annual cost of $2,995 per owner/operator for the software necessary for continuous monitoring as discussed in Section 2.4.4.8.

Table 3-15 presents continuous monitoring freight rail costs over 10 years. It includes new entity monitoring costs, existing entity monitoring costs, and software costs.

[232] TSA calculates the estimated time burden as 4 hours + 8 hours + (2 hours × 4 quarters × 4 network/systems administrators) + (15 minutes per day × 250 working days per year) ÷ 60 minutes = 62.5 hours). The total time burden is 106.5 hours in Year 1 (12 + 32 + 62.5).

[233] TSA calculates the weighted compensation rate as ($127.10 × 12 hours) + ($64.63 × 94.5 hours) ÷ 106.50 hours. Value used in analysis is rounded to two decimal places.

[234] TSA calculates the weighted compensation rate as ($127.10 × 6) + ($64.63 × 94.5 hours) ÷ 100.50 hours. Value used in analysis is rounded to two decimal places.

Table 3-15: Continuous Monitoring Costs for Freight Rail ($ Thousands)

Year	New Freight Rail Affected Entities	Existing Freight Rail Affected Population	New Entity Continuous Monitoring Cost	Existing Entity Continuous Monitoring Cost	Continuous Monitoring Software Cost	Total Freight Rail Continuous Monitoring Cost
	a = Column b, Table 2-1	$b_{y1} = 0$ $b_{Yn} = a_{Yn-1} + b_{Yn-1}$	c = a × 106.5 hours × $71.67	d = b × 100.5 hours × $68.36	e = (a + b) × $2,995	f = c + d + e
1	73.00	0	$557.2	$0.0	$218.6	$775.8
2	0.57	73.00	$4.4	$501.5	$220.3	$726.2
3	0.57	73.57	$4.4	$505.4	$222.0	$731.8
4	0.58	74.14	$4.4	$509.4	$223.8	$737.6
5	0.59	74.72	$4.5	$513.3	$225.6	$743.4
6	0.59	75.31	$4.5	$517.4	$227.3	$749.2
7	0.59	75.90	$4.5	$521.4	$229.1	$755.0
8	0.60	76.49	$4.6	$525.5	$230.9	$761.0
9	0.60	77.09	$4.6	$529.6	$232.7	$766.9
10	0.61	77.69	$4.7	$533.7	$234.5	$772.9
Total			**$597.7**	**$4,657.4**	**$2,264.8**	**$7,519.9**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed. Formulas with X_{yn-1} in year one are equal to the initial value of X_{y1}.

3.1.3.8 Capabilities to Respond to a Cybersecurity Incident

This provision details additional requirements that owner/operators must include in their COIP capabilities when it comes to responding to cybersecurity incidents that affect Critical Cyber Systems. These specifics are discussed in Section 2.4.4.6 and the time necessary to address these requirements is incorporated into the overall plan development estimates, which is accounted for and discussed in Section 2.4.4.9.

3.1.3.9 Plan of Action and Milestones (POAM) Cost

Owner/operators who are unable to meet every requirement and security outcome required by the COIP must create a POAM that includes policies, procedures, measures, or capabilities that the owner/operator will develop to ensure all requirements are met. Due to the constantly changing cybersecurity environment, TSA expects a portion of owner/operators would be unable to meet every requirement and security outcome each year and would be required to complete a POAM. As a result of existing voluntary frameworks and compliance with the SDs, TSA estimates 20

percent of owner/operators would need to complete a POAM in the first three years of the rule and that it would take 80 hours to complete (see Section 2.4.4.10). TSA invites comment on the proportion of owner/operators who would need to complete a POAM. TSA SMEs with cybersecurity expertise estimate a network/systems administrator would spend 48 hours on this task while a cybersecurity analyst would spend 32 hours.

TSA calculates a weighted average compensation rate of $65.71 per hour using the fully-loaded wage rate for a network/systems administrator of $64.63 and of $67.34 per hour for the cybersecurity analyst.[235]

TSA multiplies average compensation rate by the POAM hour burden (80 hours) and the affected Freight Rail entity population to yield the 10-year POAM cost, as shown in Table 3-16 below.

Table 3-16: POAM Costs for Freight Rail ($ Thousands)

Year	Freight Rail Population	Freight Rail Affected Population	Total POAM Cost for Freight Rail
	a = Column a, Table 2-1	b = {a × 20%, 0}	c = b × 80 hours × $65.71
1	73.00	14.60	$76.7
2	73.57	14.71	$77.3
3	74.14	14.83	$78.0
4	74.72	0	$0.0
5	75.31	0	$0.0
6	75.90	0	$0.0
7	76.49	0	$0.0
8	77.09	0	$0.0
9	77.69	0	$0.0
10	78.30	0	$0.0
Total			**$232.0**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

3.1.3.10 Total Cost of the COIP

TSA estimates the total cost impact of all COIP components for freight rail entities as $942

[235] TSA calculates the weighted compensation rate as ($64.63 × 48 hours) + ($67.34 × 32 hours) ÷ 80 hours. Value used in analysis is rounded to two decimal places.

million undiscounted over 10 years as presented in Table 3-17 below.

The table also presents the total cost of each provision as a percent of total COIP costs. The cost of MFA use represents the largest share of COIP costs at 48.3 percent, largely in part because this cost recurs daily and is driven by employee population.

Table 3-17: Total COIP Cost for Freight Rail ($ Thousands)

Year	COIP Development and Accountable Executive Designation	Cybersecurity Coordinator Designation	Identification of Critical Cyber Systems	Supply Chain Risk Management	Network Segmentation	Access Control			Patching	Critical System Data Backups	Cybersecurity Training	Detection of Cybersecurity Incidents	POAM	Total Cost of the COIP for Freight Rail
						Compliance	MFA Equipment	MFA Implementation						
	a = Table 3-4	c = Table 3-5	d = Table 3-6	e = Table 3-7	f = Table 3-8	g = Table 3-9	h = Column b, Table 3-10	i = Column c, Table 3-10	j = Table 3-11	k = Table 3-13	l = Table 3-13 + Table 3-14	m = Table 3-15	n = Table 3-16	
1	$404.0	$37.6	$1,129.2	$2,356.7	$5,457.4	$778.5	$8,421.1	$44,605.3	$7,482.1	$12,071.0	$10,485.5	$775.8	$76.7	$94,080.9
2	$129.5	$1.8	$291.1	$2,375.1	$4,015.5	$398.0	$8,456.5	$44,792.6	$7,522.0	$12,443.7	$9,789.9	$726.2	$77.3	$91,019.3
3	$130.5	$1.8	$293.3	$2,393.5	$4,046.6	$401.1	$8,492.0	$44,980.8	$7,580.2	$12,827.1	$9,831.0	$731.8	$78.0	$91,787.7
4	$131.5	$1.8	$295.7	$2,412.3	$4,078.3	$404.2	$8,527.7	$45,169.7	$7,639.5	$13,223.3	$9,872.4	$737.6	$0.0	$92,494.0
5	$132.6	$1.9	$298.1	$2,431.3	$4,110.6	$407.5	$8,563.5	$45,359.4	$7,699.9	$13,632.9	$9,913.9	$743.4	$0.0	$93,294.9
6	$133.6	$1.9	$300.4	$2,450.3	$4,142.7	$410.6	$8,599.5	$45,549.9	$7,760.2	$14,054.2	$9,955.5	$749.2	$0.0	$94,108.1
7	$134.6	$1.9	$302.6	$2,469.4	$4,174.9	$413.8	$8,635.6	$45,741.2	$7,820.5	$14,487.8	$9,997.3	$755.0	$0.0	$94,934.6
8	$135.7	$1.9	$305.1	$2,488.8	$4,207.7	$417.1	$8,671.8	$45,933.3	$7,881.8	$14,935.8	$10,039.4	$761.0	$0.0	$95,779.5
9	$136.7	$1.9	$307.4	$2,508.1	$4,240.4	$420.3	$8,708.3	$46,126.3	$7,943.2	$15,396.8	$10,081.5	$766.9	$0.0	$96,637.8
10	$137.8	$1.9	$309.9	$2,527.8	$4,273.8	$423.6	$8,744.8	$46,320.0	$8,005.6	$15,873.1	$10,123.9	$772.9	$0.0	$97,515.2
Total	**$1,606.6**	**$54.4**	**$3,832.8**	**$24,413.4**	**$42,748.0**	**$4,474.7**	**$85,820.7**	**$454,578.6**	**$77,335.0**	**$138,945.7**	**$100,090.4**	**$7,519.9**	**$232.0**	**$941,652.1**
% of Total	0.2%	0.0%	0.4%	2.6%	4.5%	0.5%	9.1%	48.3%	8.2%	14.8%	10.6%	0.8%	0.0%	100.00%

3.1.4 Reporting Cybersecurity Incidents Cost

Under the proposed rule, owner/operators would be required to report any cybersecurity incident, as defined in the TSA Cybersecurity Lexicon, to CISA as soon as practicable, but no later than 24 hours after a cybersecurity incident is identified. The reporting entity must include the contact information of the reporting individual, the affected systems, a description of the incident and threat, earliest known date of compromise, date of detection and other relevant information. A TSA SME with cybersecurity expertise utilizes internal data relating to reportable incidents to estimate 0.14 expected freight rail cybersecurity incidents requiring reporting a year per owner/operator as discussed in Section 2.4.10. TSA estimates that each affected entity would incur a one hour time burden to report each incident.[236] TSA expects the one hour time burden would be split equally between a cybersecurity analyst and COM. TSA calculates a weighted average compensation rate of $97.22 per hour using a fully-loaded wage rate for a cybersecurity analyst of $67.34 and for a COM of $127.10 per hour from Section 2.3.1.[237] TSA then multiplies the weighted average compensation rate ($97.22) by the incident reporting hour burden (1 hour) number of freight railroads per year, and expected incident reporting volume to calculate a freight rail cybersecurity incident reporting costs.

Table 3-18 presents the total freight rail cybersecurity incident reporting cost over 10 years.

[236] Time burden sourced from 1652-0051 Rail Transportation for Incident Reporting ICR. TSA estimates the hour burden for reporting an incident would be similar to the significant security concern hour burden as documented in the Supporting Statement of this ICR. See page 9.

[237] TSA calculates the weighted compensation rate as (($127.10 × 0.5 hours) + ($67.34 × 0.5 hours)) ÷ 1 hour. Value used in analysis is rounded to two decimal places.

Table 3-18: Cybersecurity Incident Reporting Cost for Freight Rail ($ Thousands)

Year	Freight Rail Population	Number of Cybersecurity Incidents Reported	Cost to Report Incidents
	a = Column a, Table 2-1	b = a × 0.14	c = b × 1 hour × $97.22
1	73.00	10.22	$1.0
2	73.57	10.30	$1.0
3	74.14	10.38	$1.0
4	74.72	10.46	$1.0
5	75.31	10.54	$1.0
6	75.90	10.63	$1.0
7	76.49	10.71	$1.0
8	77.09	10.79	$1.1
9	77.69	10.88	$1.1
10	78.30	10.96	$1.1
Total			**$10.3**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

3.1.5 Cybersecurity Incident Response Plan (CIRP) Cost

Under the proposed rule, each affected owner/operator must develop and maintain a CIRP to be filed with TSA. The CIRP must provide specific measures to ensure prompt isolation and segregation of the infected system from the uninfected systems, address the security and integrity of backed-up data, establish capability and governance for implementing mitigation measures, identify which individual is responsible for implementing the CIRP, and conduct exercises to test the plan's effectiveness. TSA estimates the COM of each affected owner/operator would spend 80 hours in Year 1 to develop the plan and 20 hours in each subsequent year to maintain the plan. TSA multiplies the COM fully-loaded wage rate of $127.10 discussed in Section 2.3.1 by CIRP development time burden (80 hours) and number of new freight rail entities to estimate CIRP development costs. TSA multiplies the same wage rate by the CIRP maintenance hour burden (20 hours) and number of existing freight railroads to calculate CIRP maintenance costs. Table 3-19 presents freight rail CIRP costs over 10 years. It includes initial CIRP development costs and CIRP annual maintenance costs.

In addition, TSA estimates owner/operators would spend an average of 120 hours to test the effectiveness of their CIRP as discussed in Section 2.4.4.5. TSA assumes this testing would be

completed by the equivalent of a COM. TSA multiplies the fully loaded COM wage rate of $127.10 per hour from Section 2.3.1, CIRP effectiveness testing hour burden (120 hours), and number of freight rail owner/operators to calculate CIRP effectiveness testing costs per year.

Table 3-19: Cybersecurity Incident Response Plan (CIRP) Costs for Freight Rail ($ Thousands)

Year	New Freight Rail Affected Entities	Existing Freight Rail Affected Population	New Entity CIRP Cost	Existing Entity CIRP Cost	CIRP Effectiveness Testing Cost	Total CIRP Cost
	a = Column b, Table 2-1	$b_{y1} = 0$ $b_{Yn} = a_{Yn-1} + b_{Yn-1}$	c = a × 80 hours × $127.10	d = b × 20 hours × $127.10	e = (a + b) × 120 hours × $127.10	f = c + d + e
1	73.00	0.00	$742.3	$0.0	$1,113.4	$1,855.7
2	0.57	73.00	$5.8	$185.6	$1,122.1	$1,313.5
3	0.57	73.57	$5.8	$187.0	$1,130.8	$1,323.6
4	0.58	74.14	$5.9	$188.5	$1,139.6	$1,334.0
5	0.59	74.72	$6.0	$189.9	$1,148.6	$1,344.6
6	0.59	75.31	$6.0	$191.4	$1,157.6	$1,355.1
7	0.59	75.90	$6.0	$192.9	$1,166.6	$1,365.6
8	0.60	76.49	$6.1	$194.4	$1,175.8	$1,376.3
9	0.60	77.09	$6.1	$196.0	$1,184.9	$1,387.0
10	0.61	77.69	$6.2	$197.5	$1,194.2	$1,397.9
Total			**$796.2**	**$1,723.2**	**$11,533.7**	**$14,053.1**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed. Formulas with X_{yn-1} in year one are equal to the initial value of X_{y1}.

In addition, each entity would implement its CIRP following a cyber-incident. TSA estimates each entity would spend 160 hours per incident to implement its CIRP as discussed in Section 2.4.6. TSA estimates 60 percent of the hour burden would be performed by a network/systems administrator and 40 percent of the hour burden would be performed by a cybersecurity analyst.[238] TSA calculates a weighted average compensation rate of $65.71 per hour using a fully-loaded wage for a cybersecurity analyst of $67.34 per hour and for a network/systems administrator of $64.63 per hour as discussed in Section 2.3.1.[239] TSA multiplies the weighted

[238] TSA SMEs with cybersecurity expertise estimate time burdens as (160 hours × 0.60 = 96 hours) and (160 hours × 0.40 = 64 hours).

[239] TSA calculates the weighted compensation rate as ($64.63 × 96 hours) + ($67.34 × 64 hours) ÷ 160 hours. Value used in analysis is rounded to two decimal places.

average compensation rate ($65.71) by the CIRP implementation hour burden (160 hours) and the number of freight railroads cybersecurity incidents per year to calculate freight rail CIRP costs.

Table 3-20: Cybersecurity Incident Response Plan (CIRP) Implementation Costs for Freight Rail ($ Thousands)

Year	Freight Rail Population	Number of Cybersecurity Incidents	Cost to Respond to Incidents
	a = Column a, Table 2-1	b = a × 0.14	c = b × 160 hours × $65.71
1	73.00	10.22	$107.4
2	73.57	10.30	$108.3
3	74.14	10.38	$109.1
4	74.72	10.46	$110.0
5	75.31	10.54	$110.8
6	75.90	10.63	$111.7
7	76.49	10.71	$112.6
8	77.09	10.79	$113.5
9	77.69	10.88	$114.4
10	78.30	10.96	$115.3
Total			**$1,113.1**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

3.1.6 Cybersecurity Assessment Plan (CAP) Cost

Under the proposed rule, each owner/operator must develop and maintain a Cybersecurity Assessment Plan (CAP) to be filed with and approved by TSA. The CAP must proactively assess the effectiveness of the COIP, and identify and resolve vulnerabilities associated with identified Critical Cyber Systems, including device, network, or other identified vulnerabilities. TSA estimates that the equivalent of a cybersecurity analyst would spend 40 hours to develop the CAP and a COM and network/systems administrator will each spend two hours reviewing the CAP.[240]

TSA calculates a weighted average compensation rate of $69.93 per hour using the fully-loaded wage rate for a COM of $127.10, a cybersecurity analyst of $67.34, and a network/systems

[240] TSA SMEs with cybersecurity expertise estimate the time burden as 40 hours for the cybersecurity analyst + (2 hours × 2 cybersecurity coordinators) = 44 total hours.

administrator of $64.63 per hour as discussed in Section 2.3.1.[241] TSA multiplies the average compensation rate by the CAP creation hour burden (44 hours) and the freight rail entity population as shown in Table 3-19 below.

In addition, each entity would implement its CAP by conducting architectural design review (ADR) and penetration testing every two years, beginning in Year 2. While penetration testing is not a stated rule requirement, TSA is including representative costs to reflect actions that may be taken by companies as a part of their processes to be in full compliance with the provisions of the proposed rule in pursuit of a strong CRM program. TSA estimates each entity would conduct penetration testing upon its second full year in the population. TSA estimates each entity would spend 40 hours to implement the CAP and conduct the ADR, with 24 hours attributed to the network/systems administrator and 16 hours attributed to the cybersecurity analyst as discussed in Section 2.4.7. TSA estimates that in addition to the ADR time burden, each entity would incur a flat cost of $20,000 every two years to conduct penetration testing.[242] TSA estimates each entity would only conduct ADR and penetration testing every 2 years. TSA assumes existing entities would conduct such activities in the 2nd full year after the implementation of the rule. In years between these periods, no existing entities would conduct activities.

TSA calculates a weighted average compensation rate of $65.71 per hour using the fully-loaded wage rate for a cybersecurity analyst of $67.34 and for a network/systems administrator of $64.63 per hour as discussed in Section 2.3.1.[243]

---

[241] TSA calculates the weighted compensation rate as ($67.34 × 40 hours) + ($127.10 × 2 hours) + ($64.63 × 2 hours) ÷ 44 hours. Value used in analysis is rounded to two decimal places.
[242] RSI Security. What Is The Average Cost Of Penetration Testing?. May 5, 2023, available at https://blog.rsisecurity.com/what-is-the-average-cost-of-penetration-testing/. Accessed September 25, 2023.
[243] TSA calculates the weighted compensation rate as ($67.34 × 8 hours) + ($64.63 × 12 hours) ÷ 20 hours. Value used in analysis is rounded to two decimal places.

TSA calculates the cost of ADR using the previously described compensation rate multiplied by the ADR hour burden (40 hours) and ADR two-year cycle. TSA similarly estimates penetration testing by multiplying the two-year cycle by the cost of penetration testing ($20,000). Table 3-21 below presents freight rail CAP costs over 10 years.

Table 3-21: Cybersecurity Assessment Plan (CAP) Cost for Freight Rail ($ Thousands)

Year	Freight Rail Affected Population	Initial Population ADR & Penetration Testing Cycle	Annual New Entity Growth	New Entities ADR & Penetration Testing Cycle	Total Entities Conducting Penetration Tests	Cost to Develop CAP	Cost of ADR & Penetration Testing	Total CAP Cost
	a = Column a, Table 2-1	b = {0, a_{y1}}	c = a_{yn} - a_{yn-1}	d = c_{n-1} + d_{n-2}	e = b + d	f = a × 44 hours × $69.93	g = (e × 40 hours × $65.71) + (e × $20,000)	h = f + g
1	73.00	0.00			0.00	$224.6	$0.0	$224.6
2	73.57	73.00	0.57	0.00	73.00	$226.4	$1,651.9	$1,878.2
3	74.14	0.00	0.57	0.57	0.57	$228.1	$12.9	$241.0
4	74.72	73.00	0.58	0.57	73.57	$229.9	$1,664.8	$1,894.7
5	75.31	0.00	0.59	1.15	1.15	$231.7	$26.0	$257.7
6	75.90	73.00	0.59	1.16	74.16	$233.5	$1,678.1	$1,911.7
7	76.49	0.00	0.59	1.74	1.74	$235.4	$39.4	$274.7
8	77.09	73.00	0.60	1.75	74.75	$237.2	$1,691.5	$1,928.7
9	77.69	0.00	0.60	2.34	2.34	$239.0	$53.0	$292.0
10	78.30	73.00	0.61	2.35	75.35	$240.9	$1,705.0	$1,946.0
Total						**$2,326.8**	**$8,522.5**	**$10,849.3**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed. Formulas with X_{yn-1} in year one are equal to the initial value of X_{y1}.

The CAP must also include a schedule to ensure completion of planned assessments. The schedule must ensure at least 30 percent of the policies, procedures, measures, and capabilities in the COIP are assessed each year and 100 percent are assessed every three years. TSA SMEs with cybersecurity expertise estimate that each owner/operator would incur a time burden of 30 hours annually to test the COIP. TSA also estimates a network/systems administrator would incur 18 hours of this time, while a cybersecurity analyst would incur the remaining 12 hours. In addition to this time burden, TSA estimates that each entity would incur a flat cost of $6,667 annually, or $20,000 over three years, to test the COIP as discussed in Section 2.4.7.

TSA calculates a weighted average compensation rate of $65.71 per hour using the fully-loaded wage rate for a cybersecurity analyst of $67.34 and for a network/systems administrator of $64.63 per hour as discussed in Section 2.3.1.[244] TSA multiplies this compensation rate by COIP testing hour burden (30 hours) and the freight rail entity population to calculate COIP administrative costs. TSA then multiplies COIP testing ($6,667) by the freight rail entity population. Table 3-22 shows the total freight rail COIP testing costs over 10 years.

[244] TSA calculates the weighted compensation rate as ($67.34 × 12 hours) + ($64.63 × 18 hours) ÷ 30 hours. Value used in analysis is rounded to two decimal places.

Table 3-22: COIP Testing Cost for Freight Rail ($ Thousands)

Year	Freight Rail Population	Administrative Cost	Cost of Testing	Total COIP Testing Cost
	a = Column a, Table 2-1	b = a × 30 hour x $65.71	c = a × $6,667	d = b + c
1	73.00	$143.9	$486.7	$630.6
2	73.57	$145.0	$490.5	$635.5
3	74.14	$146.2	$494.3	$640.4
4	74.72	$147.3	$498.1	$645.4
5	75.31	$148.5	$502.1	$650.5
6	75.90	$149.6	$506.0	$655.6
7	76.49	$150.8	$509.9	$660.7
8	77.09	$152.0	$513.9	$665.9
9	77.69	$153.2	$517.9	$671.1
10	78.30	$154.4	$522.0	$676.4
Total		**$1,490.7**	**$5,041.4**	**$6,532.1**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

3.1.7 Documentation to Establish Compliance Cost

Each owner/operator would incur various recordkeeping costs, including retaining documents that would be created as part of the CRM process as well as accessing and making these documents available to TSA, as requested. TSA estimates each affected entity would spend two hours of administrative assistant time annually to meet these obligations. TSA multiplies an administrative assistant fully-loaded wage rate of $40.42, as discussed in Section 2.3.1, by the recordkeeping hour burden (2 hours) and the freight rail entity population to calculate a recordkeeping cost, as shown in Table 3-23 below.

While some of the necessary compliance parameters would be covered under specific rule provisions as part of efforts to comply with the requirements of this proposed rule, TSA additionally estimates an audit manager would incur 40 hours of time to ensure overall compliance with the full rule each year. TSA multiplies an audit manager fully-loaded wage rate of $92.65, as discussed in Section 2.3.1, by the compliance hour burden (40 hours) and the freight rail entity population to calculate a compliance cost, as shown in Table 3-23, below.

Table 3-23: Recordkeeping and Compliance Cost for Freight Rail ($ Thousands)

Year	Freight Rail Affected Population	CRM Recordkeeping (Administrative Assistant)	CRM Compliance (Audit Manager)	Total Freight Rail Recordkeeping Cost
	a = Column a, Table 2-1	b = a × 2 hours × $40.42	c = a × 40 hours × $92.65	d = b + c
1	73.00	$5.9	$270.5	$276.4
2	73.57	$5.9	$272.7	$278.6
3	74.14	$6.0	$274.8	$280.8
4	74.72	$6.0	$276.9	$283.0
5	75.31	$6.1	$279.1	$285.2
6	75.90	$6.1	$281.3	$287.4
7	76.49	$6.2	$283.5	$289.7
8	77.09	$6.2	$285.7	$291.9
9	77.69	$6.3	$287.9	$294.2
10	78.30	$6.3	$290.2	$296.5
Total		**$61.1**	**$2,802.5**	**$2,863.6**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

3.1.8 Total Cost Impact to Freight Railroads

TSA estimates the total cost impact of all proposed rule requirements for freight rail entities as $979.7 million undiscounted over 10 years, $834.5 million discounted at 3 percent, and $685.8 million discounted at 7 percent. Table 3-24 shows the total cost of the CRM program, which includes costs related to the CSE, COIP, CAP, Recordkeeping, and Compliance. In Table 3-25 TSA aggregates the various proposed rule costs cost discussed above including Familiarization; the CRM Program; Incident Reporting; and the CIRP. Table 3-25 also presents the percent of total cost for freight railroads of each cost category.

Table 3-24: Summary of CRM Program Costs - Freight Rail ($ Thousands)

Year	CSE	COIP	CAP	Recordkeeping and Compliance	Total Cost of CRM for Freight Rail
	a = Table 3-2	b = Table 3-17	c = Table 3-21 + Table 3-22	d = Table 3-23	e = ∑a,b,c,d
1	$233.2	$94,080.9	$855.2	$276.4	$95,445.8
2	$235.0	$91,019.3	$2,513.7	$278.6	$94,046.7
3	$236.8	$91,787.7	$881.4	$280.8	$93,186.7
4	$238.7	$92,494.0	$2,540.1	$283.0	$95,555.8
5	$240.6	$93,294.9	$908.3	$285.2	$94,728.9
6	$242.4	$94,108.1	$2,567.3	$287.4	$97,205.2
7	$244.3	$94,934.6	$935.4	$289.7	$96,404.1
8	$246.3	$95,779.5	$2,594.6	$291.9	$98,912.2
9	$248.2	$96,637.8	$963.1	$294.2	$98,143.2
10	$250.1	$97,515.2	$2,622.3	$296.5	$100,684.2
Total	**$2,415.6**	**$941,652.1**	**$17,381.5**	**$2,863.6**	**$964,312.8**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

Table 3-25: Summary of Proposed Rule Requirement Costs - Freight Rail ($ Thousands)

Year	Familiar-ization	CRM Program				Reporting Cybersecurity Incidents	CIRP	Total Cost		
		CSE	COIP	CAP	Recordkeeping and Compliance			h = ∑a,b,c,d,e,f,g		
	a	b	c	d	e	f	g	Undiscounted	Discounted at 3%	Discounted at 7%
1	$242.2	$233.2	$94,080.9	$855.2	$276.4	$1.0	$1,963.1	$97,652.0	$94,807.8	$91,263.6
2	$2.0	$235.0	$91,019.3	$2,513.7	$278.6	$1.0	$1,421.7	$95,471.4	$89,990.9	$83,388.4
3	$2.0	$236.8	$91,787.7	$881.4	$280.8	$1.0	$1,432.7	$94,622.4	$86,592.9	$77,240.1
4	$2.0	$238.7	$92,494.0	$2,540.1	$283.0	$1.0	$1,444.0	$97,002.7	$86,185.7	$74,002.9
5	$2.0	$240.6	$93,294.9	$908.3	$285.2	$1.0	$1,455.4	$96,187.3	$82,972.1	$68,580.3
6	$2.0	$242.4	$94,108.1	$2,567.3	$287.4	$1.0	$1,466.8	$98,675.1	$82,638.8	$65,751.4
7	$2.0	$244.3	$94,934.6	$935.4	$289.7	$1.0	$1,478.1	$97,885.3	$79,589.7	$60,958.0
8	$2.1	$246.3	$95,779.5	$2,594.6	$291.9	$1.1	$1,489.8	$100,405.1	$79,260.7	$58,436.7
9	$2.1	$248.2	$96,637.8	$963.1	$294.2	$1.1	$1,501.3	$99,647.7	$76,371.7	$54,201.8
10	$2.1	$250.1	$97,515.2	$2,622.3	$296.5	$1.1	$1,513.2	$102,200.5	$76,046.8	$51,953.6
Total	**$260.3**	**$2,415.6**	**$941,652.1**	**$17,381.5**	**$2,863.6**	**$10.3**	**$15,166.2**	**$979,749.6**	**$834,457.1**	**$685,776.6**
% of Total	0.0%	0.2%	96.1%	1.8%	0.3%	0.0%	1.5%	100%		
Annualized									**$97,823.8**	**$97,639.2**

Note: Totals may not add due to rounding. CAP costs fluctuate every other year from the two-year cycle of penetration testing and architectural design review.

3.2 Cost Impacts to Passenger Transit and Passenger Rail

This section details the costs to passenger transit and passenger rail (PTPR) owner/operators associated with the creation and maintenance of a CRM Program as detailed in the proposed rule. Section § 1582.203 details the components covered entities would be required to have in their CRM programs as well as parameters for subsidiaries. These include a cybersecurity evaluation (CSE), a TSA-approved Cybersecurity Operational Implementation Plan (COIP), a TSA-approved CIRP, and a Cybersecurity Assessment Plan (CAP) whose costs are discussed in Sections 3.2.2 (CSE), 3.2.3 (COIP), 3.2.5 (CIRP), and 3.2.6 (CAP) accordingly. Additional costs related to familiarization, reporting cybersecurity incidents, as well as recordkeeping and documentation are also included below.

3.2.1 Familiarization Cost

TSA anticipates PTPR owner/operators would incur a familiarization cost to review the proposed rule requirements and determine applicability. Familiarization cost includes the time it takes to review the proposed rule's specifications and determine what is needed to achieve compliance. TSA uses a two-pronged approach to estimate familiarization. TSA first estimates that each owner/operator across the full industry would review the applicability portion of the rule to determine if they are covered under the scope. According to data from the American Public Transportation Association, there are 92 PTPR entities in the industry.[245] TSA expects an attorney and an individual with the equivalent responsibility of the accountable executive would each spend a half hour reviewing the applicability portion of the rule, for a total burden of one

[245] American Public Transportation Association (APTA). Jan. 2023. 2022 Public Transportation Fact Book. https://www.apta.com/wp-content/uploads/APTA-2022-Public-Transportation-Fact-Book.pdf. Accessed on July 17, 2023.

hour.[246] TSA next calculates a weighted average compensation rate of $103.50 per hour using the fully-loaded wage rate for an attorney of $72.68 and accountable executive of $134.31 per hour from Section 2.3.2.[247] TSA then multiplies the weighted average compensation rate ($103.50) by the applicability determination hour burden (1 hour) and number of PTPRs per year to calculate a total PTPR applicability determination cost.

Second, for owner/operators where the rule is applicable, they would incur costs to review the proposed rule and determine what is needed to achieve compliance. TSA assumes that a COM and an attorney within covered owner/operators would review all applicable sections in Year 1 of the proposed rule with new individuals reviewing in subsequent years.[248]

TSA estimates that a COM and an attorney from each affected owner/operator would each spend 7.08 hours to review the regulation, as discussed in Section 2.4.1. TSA additionally estimates that 15 minutes of time will be taken for a COM to brief an accountable executive on the requirements of the rule.

TSA next calculates a weighted average compensation rate of $90.29 per hour using the fully-loaded wage rate for a COM of $105.82, an attorney of $72.68, and accountable executive of $134.31 per hour.[249] TSA then multiplies the weighted average compensation rate by the rule review hour burden (14.66 hours) to calculate a PTPR rule review cost. Table 3-26 presents the

---

[246] TSA estimates this as a small hour burden based upon the applicability section being short (less than one page) and the reader's inherent knowledge of their company.
[247] TSA calculates the weighted compensation rate as (($72.68 × 0.5 hours) + ($134.31 × 0.5 hours)) ÷ 1 hour. Value used in analysis is rounded to two decimal places.
[248] See Section 2.1.2.
[249] TSA calculates the total time burden as 14.66 = (7.08 hours × 2) + 0.25 hours + 0.25 hours. TSA calculates the weighted compensation rate as (($134.31 × 0.25 hours) + ($105.82 × 7.33 hours) + ($72.68 × 7.08 hours)) ÷ 14.66 hours. Value used in analysis is rounded to two decimal places.

total PTPR familiarization cost over time. It includes applicability determination and rule review costs.

Table 3-26: Cost of the Rule Familiarization for PTPR ($ Thousands)

Year	Total PTPR Population Growth	Applicability Determination Cost	PTPR Affected Population plus Growth	Rule Review Cost	Total PTPR Familiarization Cost
	a = (92 × (1 + 2.19%) ^ (Y_{n-1})) - ∑($a_{Y1...}$ a_{Yn} – 1)	b = a × 1 hour × $103.50	c = Column e, Table 2-1	d = c × 14.66 hours × $90.29	e = b + d
1	92.00	$9.5	34.00	$45.0	$54.5
2	2.01	$0.2	0.74	$1.0	$1.2
3	2.06	$0.2	0.77	$1.0	$1.2
4	2.11	$0.2	0.77	$1.0	$1.2
5	2.15	$0.2	0.80	$1.1	$1.3
6	2.20	$0.2	0.81	$1.1	$1.3
7	2.24	$0.2	0.83	$1.1	$1.3
8	2.29	$0.2	0.85	$1.1	$1.4
9	2.35	$0.2	0.86	$1.1	$1.4
10	2.40	$0.2	0.89	$1.2	$1.4
Total		**$11.6**		**$54.7**	**$66.3**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed. Formulas with X_{yn-1} in year one are equal to the initial value of X_{y1}.

3.2.2 Cybersecurity Evaluation (CSE) Cost

The CSE provision requires that each owner/operator required to have a CRM program complete an initial and recurrent cybersecurity evaluation. The cost of this requirement relates to the time burden for entities to conduct the evaluation as well as any costs incurred to immediately address risks identified. TSA SMEs with cybersecurity expertise first estimates an annual average time to conduct this evaluation of 40 hours annually, which includes 30 hours of a cybersecurity analyst time and 10 hours of a network/systems administrator's time.

TSA next calculates a weighted average compensation rate of $63.27 per hour using the fully-loaded wage rate for a cybersecurity analyst of $63.15 and network/systems administrator of

$63.63 per hour as discussed in Section 2.3.2.[250] TSA then multiplies the weighted average compensation rate ($63.27) by the evaluation hour burden (40 hours) and number of PTPRs per year to calculate PTPR evaluation costs per year.

Next, TSA assumes some entities would choose to immediately plan how to address some of the risk areas discovered while others would wait to address risks through their COIP. Surface transportation SMEs estimate that 20 percent of owner/operators would begin to plan to address risks immediately upon completion of their evaluation. TSA assumes that such efforts would occur each year following the evaluation and that a cybersecurity analyst and network/systems administrator would each spend an average of 20 hours planning to address identified risks for a total of 40 hours.[251] TSA next calculates a weighted average compensation rate of $63.39 per hour using the fully-loaded wage rate for a cybersecurity analyst of $63.15 and network/systems administrator wage rate of $63.63 per hour. TSA then multiplies the weighted average compensation rate ($63.39) by the evaluation risk reduction hour burden (40 hours), percent of owner/operators who take action (20 percent), and number of PTPRs per year to calculate a PTPR evaluation risk reduction cost. [252]

Table 3-27 presents the total PTPR CSE cost over 10 years. It includes cybersecurity evaluation and risk reduction costs.

[250] TSA calculates the weighted compensation rate as ($63.15 × 30) hours + ($63.63 × 10 hours) ÷ 40 hours. Value used in analysis is rounded to two decimal places.
[251] TSA calculates the estimated time burden as twenty (20) hours for a cybersecurity analyst + twenty (20) hours for network/systems administrator = forty (40) hours total.
[252] TSA calculates the weighted compensation rate as ($63.15 × 20 hours) + ($63.63 × 20 hours) ÷ 40 hours. Value used in analysis is rounded to two decimal places.

Table 3-27: Cybersecurity Evaluation (CSE) Cost for PTPR ($ Thousands)

Year	PTPR Affected Population	CSE Annual Evaluation Cost	Implementation Population	CSE Implementation Cost	Total CSE Cost
	a = Column d, Table 2-1	b = a × 40 hours × $63.27	c = a × 20%	d = c × 40 hours × $63.39	e = b + d
1	34.00	$86.0	6.80	$17.2	$103.3
2	34.74	$87.9	6.95	$17.6	$105.5
3	35.51	$89.9	7.10	$18.0	$107.9
4	36.28	$91.8	7.26	$18.4	$110.2
5	37.08	$93.8	7.42	$18.8	$112.7
6	37.89	$95.9	7.58	$19.2	$115.1
7	38.72	$98.0	7.74	$19.6	$117.6
8	39.57	$100.1	7.91	$20.1	$120.2
9	40.43	$102.3	8.09	$20.5	$122.8
10	41.32	$104.6	8.26	$20.9	$125.5
Total		**$950.4**		**$190.4**	**$1,140.9**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed. Formulas with X_{yn-1} in year one are equal to the initial value of X_{y1}.

3.2.3 Cybersecurity Operational Implementation Plan (COIP) Cost

Each owner/operator required to have a CRM program must adopt a Cybersecurity Operational Implementation Plan (COIP). The development and implementation of one's COIP involves a level of governance that includes, identifying information about the owner/operator, including an accountable executive responsible for the sustainment of the company's cybersecurity program and providing a written attestation that the plan has been reviewed and identification of operations which meet the applicability requirements. The COIP also requires owner/operators to address specific content, including the designation of cybersecurity coordinators, identification of Critical Cyber Systems requiring protection, creating policies and procedures to protect Critical Cyber Systems, detect cybersecurity incidents, and to respond to detected cybersecurity incidents. The COIP also requires owner/operators to develop and implement cybersecurity training for general and IT specialist populations, develop standards for ensuring supply chain risk management, backup Critical Cyber Systems, and develop capabilities to respond to a cybersecurity incident. Furthermore, to the extent that the owner/operator does not meet the requirements mentioned above, owner/operator must create a plan of action and milestones

(POAM) to achieve those outcomes. The costs associated with these COIP requirements are detailed in subsections below.

3.2.3.1 Governance of the CRM Program Cost

TSA estimates owner/operators would spend 40 hours setting up an initial COIP in Year 1 and providing identifying information as discussed in Section 2.4.4. For years 2-10, TSA assumes owner/operators would spend 40 hours, in any one year in a three-year period, presented as an annual average of 13.33 hours. TSA assumes time spent on this requirement would be evenly split between a COM and a corporate attorney. TSA calculates a weighted average compensation rate of $89.25 per hour using the fully-loaded wage rate for an attorney of $72.68 and of $105.82 per hour for the COM. [253] TSA then multiplies the weighted average compensation rate ($89.25) by the COIP development hour burden (40 hours) and number of affected PTPR entities per year to calculate a PTPR COIP development cost in Year 1. TSA then multiplies the weighted average compensation rate ($89.25) by the subsequent year COIP development burden (13.33 hours) and number of affected PTPR entities per year to calculate a PTPR COIP development cost in Years 2-10.

In addition, owner/operators must identify an accountable executive of the organization responsible for the sustainment of the company's cybersecurity program and have final approval authority over program parameters. The cost of this requirement is the time it takes each affected owner/operator to identify such executive-level individual(s).[254] Given the complexity of CRM

[253] TSA calculates the weighted compensation rate as ($105.82 × 20 hours) + ($72.68 × 20 hours) ÷ 40 hours. Value used in analysis is rounded to two decimal places.

[254] TSA incorporates time for the accountable executive to review the components of the CRM program, including the COIP, CSE, CAP, Cybersecurity Training Plans and CIRP as discussed in the sections below. The accountable executive is allocated 4 hours to review the COIP for compliance and adequacy, 4 hours for training plan review.

programs, TSA recognizes that some entities may require more than one individual to hold this designation but for purposes of this analysis, has assumed that affected owner/operators will select one individual in order to meet the requirements of the rule as shown in Table 3-28.

Table 3-28: Accountable Executive Population for PTPR

Year	PTPR Population	Number of Initial Accountable Executives	Number of Additional Accountable Executives Resulting from Employee Turnover	Total Number of Accountable Executives
	a = Column d, Table 2-1	$b_{y1} = a_{y1}$ $b_{yn} = a_{yn} - a_{yn-1}$	$c_{y1} = 0$ $c_{yn} = a_{yn} \times 12.96\%$	d = b + c
1	34.00	34.00	0.00	34.00
2	34.74	0.74	4.50	5.24
3	35.51	0.77	4.60	5.37
4	36.28	0.77	4.70	5.47
5	37.08	0.80	4.81	5.61
6	37.89	0.81	4.91	5.72
7	38.72	0.83	5.02	5.85
8	39.57	0.85	5.13	5.98
9	40.43	0.86	5.24	6.10
10	41.32	0.89	5.36	6.25
Total		**41**	**44**	**86**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed. Formulas with X_{yn-1} in year one are equal to the initial value of X_{y1}.

TSA estimates owner/operators would spend three hours making this determination per identified individual, split between one hour of COM time to make the designation and two hours of attorney time to review and document the qualifying criteria. TSA next calculates a weighted average compensation rate of $83.73 per hour using the fully-loaded wage rate for a COM of $105.82 and attorney of $72.68 per hour.[255]

In addition, TSA estimates an accountable executive's turnover rate of 13 percent, based on BLS data, that would necessitate a new designation.[256] TSA then multiplies the number of accountable

[255] TSA calculates the weighted compensation rate as ($72.68 × 2 hours) + ($105.82 × 1 hours) ÷ 3 hours. Value used in analysis is rounded to two decimal places.
[256] See Section 2.2.

executives, the hour burden per accountable executive, and the weighted average compensation wage to determine the accountable executive designation cost for entities. The total accountable executive designation cost is presented in Table 3-29.

Table 3-29: COIP Governance Cost for PTPR ($ Thousands)

Year	New PTPR Entities	Existing PTPR Population	COIP Development	PTPR Accountable Executive Population	Accountable Executive Designation Cost	PTPR Total COIP Governance Cost
	a = Column e, Table 2-1	$b_{Y1} = 0$ $b_{Yn} = a_{Yn-1} + b_{Yn-1}$	c = (a × 40 hours × $89.25) + (b × 13.33 hours × $89.25)	d = Column d, Table 3-28	e = d × 3 hours × $83.73	f = c + e
1	34.00	0.00	$121.4	34.00	$8.5	$129.9
2	0.74	34.00	$43.1	5.24	$1.3	$44.4
3	0.77	34.74	$44.1	5.37	$1.3	$45.4
4	0.77	35.51	$45.0	5.47	$1.4	$46.4
5	0.80	36.28	$46.0	5.61	$1.4	$47.4
6	0.81	37.08	$47.0	5.72	$1.4	$48.4
7	0.83	37.89	$48.0	5.85	$1.5	$49.5
8	0.85	38.72	$49.1	5.98	$1.5	$50.6
9	0.86	39.57	$50.1	6.10	$1.5	$51.7
10	0.89	40.43	$51.3	6.25	$1.6	$52.8
Total			**$545.1**		**$21.5**	**$566.6**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed. Formulas with X_{yn-1} in year one are equal to the initial value of X_{y1}.

3.2.3.2 Cybersecurity Coordinator Cost

This provision requires owner/operators to provide in writing to TSA the names, titles, phone number(s), and email address(es) of the Cybersecurity Coordinator and alternate Cybersecurity Coordinator(s) within seven days of the commencement of new operations or change in any of the information required by this section. The cost of this requirement is the time each entity takes to designate a cybersecurity coordinator and alternate and to submit that information to TSA. TSA estimates all covered owner/operators would provide this information in Year 1 of the proposed rule; thereafter, covered owner/operators will need to provide updated information to account for turnover or changes in names, titles, phone number(s), or email address(es) each year. TSA estimates a 12.96 percent turnover rate as discussed in Section 2.2.

Each owner/operator vets the qualifications of the cybersecurity coordinator to determine if they meet the requirements of the role. TSA estimates that all entities would have two individuals filling this role of coordinator and alternate. TSA estimates that a COM will take 15 minutes of time to designate the cybersecurity coordinator, each designated cybersecurity coordinator would take 45 minutes of their time to provide contact details to TSA, and an attorney would spend one hour of time to review, select, and vet the identified individual to ensure the qualifications of the designated individuals. This results in a total of two hours per designation. TSA next calculates a weighted average compensation rate of $89.25 per hour using the fully-loaded wage rate for a cybersecurity coordinator of $105.82, for a COM of $105.82, and for an attorney of $72.68.[257] TSA then multiplies the number of cybersecurity coordinators by the hour burden per entity, and the weighted average compensation rate ($89.25) to determine the cybersecurity coordinator cost for PTPR as presented in Table 3-30.

[257] TSA calculates the weighted compensation rate as ($72.68 × 1 hour) + ($105.82 × 0.25 hours) + ($105.82 × 0.75 hours) ÷ 2 hours. Value used in analysis is rounded to two decimal places.

Table 3-30: Cybersecurity Coordinator Cost for PTPR ($ Thousands)

Year	PTPR Population	Number of Initial Cybersecurity Coordinators	Number of Additional Cybersecurity Coordinators Resulting From Employee Turnover	Total Number of Cybersecurity Coordinators	PTPR Cybersecurity Coordinator Cost
	a = Column d, Table 2-1	$b_{y1} = a_{y1} \times 2$ $b_{yn} = (a_{yn} - a_{yn-1}) \times 2$	$c_{y1} = 0$ $c_{yn} = a_{yn} \times 2 \times 12.96\%$	d = b + c	e = d × 2 hours × $89.25
1	34.00	68.00	0.00	68.00	$12.1
2	34.74	1.48	9.00	10.48	$1.9
3	35.51	1.54	9.20	10.74	$1.9
4	36.28	1.54	9.40	10.94	$2.0
5	37.08	1.60	9.61	11.21	$2.0
6	37.89	1.62	9.82	11.44	$2.0
7	38.72	1.66	10.04	11.70	$2.1
8	39.57	1.70	10.26	11.96	$2.1
9	40.43	1.72	10.48	12.20	$2.2
10	41.32	1.78	10.71	12.49	$2.2
Total		**83**	**89**	**171**	**$30.6**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed. Formulas with X_{yn-1} in year one are equal to the initial value of X_{y1}.

3.2.3.3 Identification of Critical Cyber Systems Costs

Under the proposed rule, owner/operators must incorporate a list of Critical Cyber Systems, as defined in the TSA Cybersecurity Lexicon, into its COIP that provides, at a minimum, an identifier and system specific information, such as the system/manufacturer/designer name for each Critical Cyber System. The owner/operator must also discuss its identification methodology and provide system architecture and connection information. Affected owner/operators would incur costs to design its identification protocol, and conduct a review of its inventory to designate Critical cyber systems, and ensure such systems are defined in the TSA Cybersecurity Lexicon.[258] TSA estimates affected entities would spend an average of 160 hours in Year 1 performing these tasks and 40 hours in subsequent years (Years 2 through 10) to review and

[258] See Section III(F)(2) of the Notice of Proposed Rulemaking for information on TSA's Cybersecurity Lexicon.

update.[259] In Year 1, TSA estimates these 160 hours includes time to design the criteria, time conduct an IT and OT inventory, time create a database, time to keep it up to date, and integrating criticality designations.[260] For Years 2 through 10, TSA estimates there will be efficiency gains from experience implementing these processes as shown in Table 2-10. In Years 2 through 10 TSA estimates each entity will spend a reduced amount of time designing the criteria, conducting an IT and OT inventory, keeping the critical systems database updated, integrating criticality decisions, and network/systems administrator review time.[261] TSA assumes these tasks would be performed by the COM, network/systems administrator, and a cybersecurity analyst.

TSA calculates a weighted average compensation rate of $84.58 per hour in using the fully-loaded wage rate for a cybersecurity analyst of $63.15, for a network/system administrator of $63.63, and for a COM of $105.82 per hour.[262]

TSA uses the same wage rate for Year 1 multiplied by the new entity hour burden to identify Critical Cyber Systems (160 hours) plus the wage rate for existing entities multiplied by the existing entity hour burden (40 hours) to calculate a Critical Cyber Systems identification cost as presented in Table 3-31 below.

---

[259] TSA consulted SMEs with cybersecurity expertise and determined an hour burden range of 80 – 244 hours for Year 1 and a range of 40 – 120 hours for Years 2-10. TSA decided to use an hour burden of 160 hours for Year 1. and 40 hours for Years 2-10 to capture the fact that some entities would have hour burdens near the low and high ends of the range.

[260] TSA SMEs with cybersecurity expertise estimate the division of the hours burden would consist of 50% cybersecurity coordinator, 30% cybersecurity analyst, and 20% network/systems administrator.

[261] Similar to Year 1, TSA calculates 24.8 hours of network/system administrator review time as 40% of the sum of the other activities' time. These activities sum to 62 hours (60 + 2). TSA calculates 62 × 0.4 = 24.8 hours.

[262] TSA calculates the weighted compensation rate as ($105.82 × 160 hours × 50%) + ($63.15 × 160 hours × 30%) + ($63.63 × 160 hours × 20%). Value used in analysis is rounded to two decimal places.

Table 3-31: Identification of Critical Cyber Systems Cost for PTPR ($ Thousands)

Year	New PTPR Affected Entities	Existing PTPR Affected Population	New Entity Cost	Existing Entity Cost	Total PTPR Identification of Critical Cyber Systems Cost
	a = Column e, Table 2-1	$b_{Y1} = 0$ $b_{Yn} = a_{Yn-1} + b_{Yn-1}$	c = a × 160 hours × $84.58	d = b × 40 hours × $84.58	e = c + d
1	34.00	0.00	$460.1	$0.0	$460.1
2	0.74	34.00	$10.0	$115.0	$125.0
3	0.77	34.74	$10.4	$117.5	$128.0
4	0.77	35.51	$10.4	$120.1	$130.6
5	0.80	36.28	$10.8	$122.7	$133.6
6	0.81	37.08	$11.0	$125.4	$136.4
7	0.83	37.89	$11.2	$128.2	$139.4
8	0.85	38.72	$11.5	$131.0	$142.5
9	0.86	39.57	$11.6	$133.9	$145.5
10	0.89	40.43	$12.0	$136.8	$148.8
Total			**$559.2**	**$1,130.7**	**$1,689.9**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed. Formulas with X_{yn-1} in year one are equal to the initial value of X_{y1}.

3.2.3.4 Supply Chain Risk Management Costs

Under the proposed rule, owner/operators must incorporate into their COIP policies, procedures, and capabilities to address supply chain cybersecurity vulnerabilities. This includes ensuring all procurement documents and contracts include a requirement for the vendor or service provider to notify the owner/operator of cybersecurity incidents, vulnerabilities, and an evaluation of the cybersecurity measures implemented by vendors. In addition, owner/operators must consider the level of cybersecurity sufficient to protect against or respond to cybersecurity incidents, and mitigation measures to address risks identified by the vendor or service provider. The cost of this requirement includes the time incurred for contract renewals and updates to come into compliance, as well as the time owner/operators spend to check the goods, services, or capabilities provided by vendors or service providers to identify potential vulnerabilities. TSA estimates affected entities would spend an average of 330 hours annually to perform these tasks. This includes 10 hours of attorney time to review and update contracts and 40 hours for a team of

4 individuals to check vendor provided capabilities twice a year.[263] TSA estimates checking vendor provided capabilities would be split between a COM who will incur a time burden of 160 hours, a cybersecurity analyst who will incur 112 hours of time, and a network/systems administrator who will incur 48 hours of time.[264] TSA calculates a weighted average compensation rate of $84.20 per hour using the fully-loaded wage rate for an attorney of $72.68, for a COM of $105.82, for a cybersecurity analyst of $63.15, and for a network/systems administrator of $63.63 per hour.[265]

TSA then multiplies the weighted average compensation rate ($84.20) by the supply chain risk management hour burden (330 hours) and number of PTPRs per year to calculate a PTPR supply chain risk management cost per year as presented in Table 3-32.

Table 3-32: Supply Chain Risk Management Cost for PTPR ($ Thousands)

Year	PTPR Affected Population	Hour Burden
	a = Column d, Table 2-1	b = a × 330 hours × $84.20
1	34.00	$944.7
2	34.74	$965.3
3	35.51	$986.7
4	36.28	$1,008.1
5	37.08	$1,030.3
6	37.89	$1,052.8
7	38.72	$1,075.9
8	39.57	$1,099.5
9	40.43	$1,123.4
10	41.32	$1,148.1
Total		**$10,434.8**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed. Formulas with X_{yn-1} in year one are equal to the initial value of X_{y1}.

3.2.3.5 Protection of Critical Cyber Systems Cost

Under the proposed rule, owner/operator must incorporate into its COIP network segmentation,

[263] TSA estimates four (4) cybersecurity analysts would spend 40 hours twice a year. 4 analysts × 40 hours × 2 times a year = 320. 320 hours for the cybersecurity analysts + 10 hours for an attorney = 330 hours.
[264] TSA SMEs with cybersecurity expertise estimate the division of the hours burden would consist of 50% cybersecurity coordinator, 35% cybersecurity analyst, and 15% network/systems administrator.
[265] TSA calculates the weighted compensation rate as ($72.68 × 10 hours) + ($105.82 × 160 hours) + ($63.15 × 112 hours) + ($63.63 × 48 hours) ÷ 330 hours. Value used in analysis is rounded to two decimal places.

procedures, controls and capabilities to protect Critical Cyber Systems that are sufficient to protect against disruption of IT and OT, secure and defend zone boundaries, control access to Critical Cyber Systems to prevent unauthorized access, reduce the risk of exploitation of unpatched systems through the application of security patches and updates, ensure logging data are stored and maintained properly, ensure all Critical Cyber Systems are regularly backed up, and other policies. The cost related to network segmentation involves developing and implementing policies to properly segment OT and IT.

TSA estimates affected entities would spend 820 hours in Year 1 and 660 hours in subsequent years (Years 2 through 10) performing this task.[266] TSA estimates the 820-hour total time burden in Year 1 is comprised of 100 hours to design the criteria, 120 hours to conduct an inventory of OT, 120 hours to review OT to OT connections, 120 hours to review OT to IT connections, 120 hours to review OT connections to third parties and 240 hours to develop networking solutions to ensure OT and IT are separate.[267]

For Years 2 through 10, TSA estimates each of the above tasks would continue each year. TSA estimates components of the time burden relating to the application would remain constant and the time burden to design segmentation criteria would fall by 40 percent to 60 hours per entity per year and the time burden to design networking solutions separating IT and OT would also fall by half to 120 hours per entity per year, for a total ongoing annual time burden of 660

[266] TSA consulted SMEs with cybersecurity expertise and determined that an hour burden range of 320 – 840 hours for Year 1 and a range of 240 – 660 hours for Years 2-10. TSA decided to use an hour burden of 820 hours for Year 1 and 660 hours for Years 2-10 as it determined the upper bound represented the average time it would take for affected owner/operators to complete these tasks.

[267] TSA SMEs with cybersecurity expertise estimate the total Year 1-hour burden as 100 + 120 +120 + 120 + 120 + 240 = 820 total hours.

hours.[268] TSA assumes the equivalent of a COM would perform the design component tasks, while a network/system administrator and cybersecurity analyst would perform the application component of the requirements.

TSA calculates a weighted average compensation rate of $81.01 per hour in Year 1 using a fully-loaded wage rate for a cybersecurity analyst of $63.15, for a network/systems administrator of $63.63 per hour, and for a COM of $105.82 per hour.[269] In Years 2 through 10, TSA calculates a weighted average compensation rate of $75.00 per hour due to the lower proportion of the time burden taken up by the COM.[270]

TSA multiplies the wage rate calculated for Year 1 by the new entity network segmentation hour burden (820 hours) and adds to it the product of the Year 2 wage rate and the existing entity network segmentation hour burden (660 hours) to calculate a network segmentation cost displayed in Table 3-33 below.

[268] TSA SMEs with cybersecurity expertise estimate the hours burden for Years 2-10 as 60 + 120 + 120 + 120 + 120 + 120 = 660 total hours.
[269] TSA calculates the weighted compensation rate as ($105.82 × 340 hours) + ($63.15 × 192 hours) + ($63.63 × 288 hours) ÷ 820 hours. Value used in analysis is rounded to two decimal places.
[270] TSA calculates the weighted compensation rate as ($105.82 × 180 hours) + ($63.15 × 192 hours) + ($63.63 × 288 hours) ÷ 660 hours. Value used in analysis is rounded to two decimal places.

Table 3-33: Network Segmentation Cost for PTPR ($ Thousands)

Year	New PTPR Affected Entities	Existing PTPR Population	New Entity Cost	Existing Entity Cost	Total PTPR Network Segmentation Cost
	a = Column e, Table 2-1	$b_{Y1} = 0$ $b_{Yn} = a_{Yn-1} + b_{Yn-1}$	c = a × 820 hours × $81.01	d = b × 660 hours × $75.00	e = c + d
1	34.00	0.00	$2,258.6	$0.0	$2,258.6
2	0.74	34.00	$49.2	$1,683.0	$1,732.2
3	0.77	34.74	$51.1	$1,719.6	$1,770.8
4	0.77	35.51	$51.1	$1,757.7	$1,808.9
5	0.80	36.28	$53.1	$1,795.9	$1,849.0
6	0.81	37.08	$53.8	$1,835.5	$1,889.3
7	0.83	37.89	$55.1	$1,875.6	$1,930.7
8	0.85	38.72	$56.5	$1,916.6	$1,973.1
9	0.86	39.57	$57.1	$1,958.7	$2,015.8
10	0.89	40.43	$59.1	$2,001.3	$2,060.4
Total			**$2,744.8**	**$16,543.9**	**$19,288.7**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed. Formulas with X_{yn-1} in year one are equal to the initial value of X_{y1}.

The costs related to access control involve designing and reviewing necessary criteria and solutions. TSA estimates owner/operators would spend a time burden of 100 hours in Year 1 and 58.34 hours in subsequent years (Years 2 through 10) performing this task.[271] The time burden in Year 1 is comprised of 50 hours to design the criteria, 33 hours to conduct an access review, and 17 hours to design network solutions per entity. In Years 2 through 10, TSA SMEs with cybersecurity expertise estimate the 33 hours needed for access review continues unchanged, while the ongoing time burden for designing the criteria and designing the network solutions falls to 17 and 8 hours, respectively. TSA SMEs with cybersecurity expertise estimate these tasks would be performed by a network/systems administrator, cybersecurity analyst, and a COM.

TSA calculates a weighted average compensation rate of $91.69 per hour using a fully-loaded

[271] TSA SMEs with cybersecurity expertise estimate an hour burden range of 75 – 200 hours for Year 1 and a range of 33 - 68 hours for Years 2-10 due to the decrease in time associated with designing criteria and designing networking solutions. TSA uses an hour burden of 100 hours for Year 1 and 58.34 hours for Years 2-10 to reflect entities having hour burdens throughout the range.

wage rate for a cybersecurity analyst of $63.15, for a network/systems administrator of $63.63, and for a COM of $105.82 per hour. [272] In Years 2-10, TSA calculates a weighted average compensation rate of $81.61 due to the lower proportion of the time burden taken up by the COM. [273]

TSA multiplies the wage rate calculated for Year 1 by the new entity access control hour burden (100 hours) and adds to it the product of the Year 2 wage rate and the existing entity access control hour burden (58.34 hours) to calculate an access control cost displayed in Table 3-34 below.

Table 3-34: Access Control Compliance Costs for PTPR ($ Thousands)

Year	New PTPR Affected Entities	Existing PTPR Affected Population	New Entity Cost	Existing Entity Cost	Total PTPR Access Control Cost
	a = Column e, Table 2-1	$b_{Y1} = 0$ $b_{Yn} = a_{Yn-1} + b_{Yn-1}$	c = a × 100 hours × $91.69	d = b × 58.34 hours x $81.68	e = c + d
1	34.00	0.00	$311.7	$0.0	$311.7
2	0.74	34.00	$6.8	$161.9	$168.7
3	0.77	34.74	$7.1	$165.4	$172.5
4	0.77	35.51	$7.1	$169.1	$176.1
5	0.80	36.28	$7.3	$172.7	$180.1
6	0.81	37.08	$7.4	$176.5	$184.0
7	0.83	37.89	$7.6	$180.4	$188.0
8	0.85	38.72	$7.8	$184.4	$192.1
9	0.86	39.57	$7.9	$188.4	$196.3
10	0.89	40.43	$8.2	$192.5	$200.7
Total			**$378.9**	**$1,591.3**	**$1,970.1**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed. Formulas with X_{yn-1} in year one are equal to the initial value of X_{y1}.

As part of their plan to control access to Critical Cyber Systems and prevent unauthorized access, TSA estimates owner/operators would procure multi-factor authentication (MFA) software at a cost of $72 per employee as discussed in Section 2.4.7. TSA estimates owner/operators would

[272] TSA calculates the weighted compensation rate as ($105.82 × 67 hours) + ($63.15 × 19.8 hours) + ($63.63 × 13.2 hours) ÷ 100 hours. Value used in analysis is rounded to two decimal places.

[273] TSA calculates the weighted compensation rate as ($105.82 × 25 hours) + ($63.15 × 19.8 hours) + ($63.63 × 13.2 hours) ÷ 58 hours. Value used in analysis is rounded to two decimal places.

have to acquire access control equipment and apply it to the user accounts of all of their employees. TSA multiplies the cost of MFA acquisition by the employee population for PTPR identified in Section 2.1.2 to obtain an MFA equipment acquisition cost.

TSA also estimates each employee would incur a time burden each time the employee uses MFA and may incur additional time burdens to manage any lockouts or password resets needed. TSA estimates each employee a one minute per day time burden to use MFA for a total of 4.17 hours per year, per employee.[274] TSA assumes employees would use MFA daily to log into IT network systems such as email, chat communications, file share servers, or HR systems. Since these are systems employees engage with regularly, TSA estimates that account lockouts will be rare. TSA estimates each employee incurs a 15-minute time burden to resolve lockouts for each occurrence and estimates each employee may experience a twice every two months, for a total of 3 hours per year, per employee as discussed in Section 2.4.4.5. Together, TSA calculates each employee incurs a time burden of 7.17 hours per year due to MFA requirements. TSA estimates the cost of MFA to entities using a fully-loaded mean wage rate of $31.23 for the PTPR employee population. TSA multiplies the same wage rate by the employee MFA time burden (7.17 hours) to calculate an employee MFA engagement cost as shown in Table 3-35 below.

[274] TSA estimates 1 min per day per employee to access MFA for a total hour burden of 4.17 hours per year, per employee. (1 ÷ 60) × 250 working days per year = 4.17 hours.

Table 3-35: Access Control Implementation Cost for PTPR ($ Thousands)

Year	Affected Employee Population Plus Growth	MFA Equipment Cost	MFA Implementation Cost	Total Cost
	a = Column d, Table 2-2	b = a_{Yn} × $72	c = a_{Yn} × 7.17 hours × $31.23	d = b + c
1	299,680.00	$21,577.0	$67,104.1	$88,681.0
2	303,006.45	$21,816.5	$67,848.9	$89,665.4
3	306,369.82	$22,058.6	$68,602.1	$90,660.7
4	309,770.52	$22,303.5	$69,363.5	$91,667.0
5	313,208.98	$22,551.0	$70,133.5	$92,684.5
6	316,685.60	$22,801.4	$70,912.0	$93,713.3
7	320,200.81	$23,054.5	$71,699.1	$94,753.5
8	323,755.04	$23,310.4	$72,494.9	$95,805.3
9	327,348.72	$23,569.1	$73,299.6	$96,868.7
10	330,982.29	$23,830.7	$74,113.3	$97,944.0
Total		**$226,872.6**	**$705,570.9**	**$932,443.5**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed. Formulas with X_{yn-1} in year one are equal to the initial value of X_{y1}.

As part of their COIP, each owner/operator must develop a patch management strategy that ensures all critical security patches and updates for operating systems, applications, drivers and firmware are current. TSA estimates affected entities would spend 82 hours in Year 1 and 80 hours in Years 2 through 10 performing this task as discussed in Section 2.4.4.5. TSA estimates this time burden is comprised of four hours in Year 1 and two hours in subsequent years to create and maintain a patch strategy and 72 hours per entity per year to manage new patches. TSA SMEs with cybersecurity expertise estimate this task would be performed by the equivalent of a system/network administrator and the COM.

TSA calculates a weighted average compensation rate of $65.69 per hour in Year 1 using a fully-loaded wage rate for a network/systems administrator of $63.63 and for a COM of $105.82 per hour.[275] In Years 2-10 TSA calculates a weighted average compensation rate of $64.68 due to the

[275] TSA calculates the weighted compensation rate as ($105.82 × 4 hours) + ($63.63 × 78 hours) ÷ 82 hours. Value used in analysis is rounded to two decimal places.

lower proportion of the time burden taken up by the COM.[276]

TSA uses the same wage rate from year 1 and multiplies by the new entity patch implementation hour burden (82 hours) to yield a patch implementation cost and adds to it the product of the wage rate for existing entities in subsequent years (Years 2 – 10) and the existing entity patch implementation hour burden (80 hours) to yield a total patch implementation cost shown in Table 3-36 below. TSA also estimates additional owner/operator time burden due to responding to new patches. TSA estimates that each entity will need to apply patches in at least one cycle per quarter and that each entity will incur time burden of 375 hours to complete each cycle as discussed in Section 2.4.4.5. TSA estimates this task would be performed by a system/network administrator using a fully-loaded wage rate of $63.63 per hour. Table 3-36 presents the total PTPR patching cost over 10 years. It includes new entity patching, existing entity patching, and cost to respond to new patches.

[276] TSA calculates the weighted compensation rate as ($105.82 × 2 hours) + ($63.63 × 78 hours) ÷ 80 hours. Value used in analysis is rounded to two decimal places.

Table 3-36: Patching Implementation Cost for PTPR ($ Thousands)

Year	New PTPR Affected Entities	Existing PTPR Affected Population	New Entity Patching Cost	Existing Entity Patching Cost	Cost to Respond to New Patches	Total PTPR Patching Cost
	a = Column e, Table 2-1	$b_{y1} = 0$ $b_{Yn} = a_{Yn-1} + b_{Yn-1}$	c = a_{Yn} × 82 hours × $65.69	d = b × 80 hours × $64.68	e = (a + b) × 4 patching cycles per year × 375 hours per cycle × $63.63	f = c + d + e
1	34.00	0.00	$183.1	$0.0	$3,245.1	$3,428.3
2	0.74	34.00	$4.0	$175.9	$3,315.8	$3,495.7
3	0.77	34.74	$4.1	$179.8	$3,389.3	$3,573.2
4	0.77	35.51	$4.1	$183.7	$3,462.7	$3,650.6
5	0.80	36.28	$4.3	$187.7	$3,539.1	$3,731.1
6	0.81	37.08	$4.4	$191.9	$3,616.4	$3,812.6
7	0.83	37.89	$4.5	$196.1	$3,695.6	$3,896.2
8	0.85	38.72	$4.6	$200.4	$3,776.8	$3,981.7
9	0.86	39.57	$4.6	$204.8	$3,858.8	$4,068.2
10	0.89	40.43	$4.8	$209.2	$3,943.8	$4,157.8
Total			**$222.6**	**$1,729.4**	**$35,843.4**	**$37,795.4**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed. Formulas with X_{yn-1} in year one are equal to the initial value of X_{y1}.

Finally, TSA estimates the cost of data backups for Critical Cyber Systems includes the cost to acquire the necessary storage space for all Critical Cyber System data backed up and the time burden to supervise the backup process. TSA SMEs with cybersecurity expertise estimate an average Critical Cyber System data volume per entity in Year 1 of 500 terabytes (TB) of data.[277] TSA estimates the storage cost per TB of data backed up as $329.16 per TB per year.[278] TSA assumes entities would use a cloud-based provider to store Critical Cyber System backup data. TSA recognizes that alternatives exist and that owner/operators may choose to store their Critical

[277] TSA assumes owner/operators would purchase cloud-based storage sufficient to meet their Critical Cyber System data backup needs in advance at the beginning of each year. TSA request comment on the average amount of storage space owner/operators would need.

[278] "Cloud Storage Pricing in 2023: Everything You Need to Know." Anina Ot. Accessed September 26, 2023. https://www.enterprisestorageforum.com/cloud/cloud-storage-pricing/. TSA uses the above article's "Cloud Storage Pricing Chart" to compare five of the six (U.S.-based) cloud storage providers. The table's final row provides a per month per TB cost estimator. The article's five point estimates average to $27.43 per TB per month (($34.67 + $24.90 + $24.08 + $26.40 + $27.00) ÷ 5). TSA multiplies the per month amount by 12 months to yield an annual cost of $329.16 per TB per year.

Cyber System backup data in a different non-cloud environment. TSA invites public comment on these cost assumptions.

TSA further estimates that the volume of Critical Cyber System data held by PTPR entities would grow in Years 2 through 10. TSA calculates a compound annual growth rate of Critical Cyber System data volume of 2.3 percent per year between Years 2 through 10.[279] Once the backup is complete, the data will need to be safely stored. TSA cybersecurity SMEs estimate that each backup will need to be stored for a period of one year. TSA scales the per TB per month cost above to reflect an annual cost.[280] TSA also estimates the cost associated with the time burden on PTPR entities to supervise the backup of their data. TSA SMEs with cybersecurity expertise estimate that each entity would require 12 hours per year (1 hour per month) to supervise the backup of their Critical Cyber System data. TSA calculates a fully loaded wage for a network/systems administrator of $63.63 per hour to supervise the backup of Critical Cyber System data.

TSA multiplies the network/systems administrator wage rate by the backup supervision hour burden (12 hours) to yield a data backup supervision cost. Table 3-37 presents PTPR critical system backup costs over time. It includes cost of data storage and time for backup supervision.

---

[279] Alex Woodie. "Big Growth Forecasted for Big Data.".https://www.datanami.com/2022/01/11/big-growth-forecasted-for-big data/#:~:text=From%202020%20to%202025%2C%20IDC,of%20data%20creation%20by%202025. Accessed July 3, 2023. TSA extracted a forecast that raw data creation is expected to grow at a compound annual rate of 23% per year per entity between 2020 and 2025. However, the author also notes that organizations only save into long-term storage roughly 10% of the data which they create each year. Therefore, the net compound annual growth rate applicable to data storage needs is 23% × 10% = 2.3% per year. TSA understands this average may not capture the exact circumstances for all industries. TSA invites public comment on this input.

[280] "Cloud Storage Pricing in 2023: Everything You Need to Know." Anina Ot. Accessed September 26, 2023. https://www.enterprisestorageforum.com/cloud/cloud-storage-pricing/

Table 3-37: Critical System Data Backups for PTPR ($ Thousands)

Year	PTPR Affected Population	Critical System Data Size Per Entity (Terabytes)	Cost of Data Backups	Cost of Data Backup Supervision	Total Cost of PTPR Critical System Data Backups
	a = Column d, Table 2-1	b_{y1} = 500 $b_{yn} = b_{yn-1} \times (1 + 2.30\%)$	c = a × b × $329.16	d = a × 12 hours × $63.63	e = c + d
1	34.00	500.00	$5,595.7	$26.0	$5,621.7
2	34.74	511.50	$5,849.0	$26.5	$5,875.5
3	35.51	523.26	$6,116.1	$27.1	$6,143.2
4	36.28	535.29	$6,392.4	$27.7	$6,420.1
5	37.08	547.60	$6,683.6	$28.3	$6,711.9
6	37.89	560.19	$6,986.6	$28.9	$7,015.5
7	38.72	573.07	$7,303.8	$29.6	$7,333.4
8	39.57	586.25	$7,635.8	$30.2	$7,666.0
9	40.43	599.73	$7,981.2	$30.9	$8,012.0
10	41.32	613.52	$8,344.4	$31.6	$8,376.0
Total			**$68,888.7**	**$286.7**	**$69,175.4**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed. Formulas with X_{yn-1} in year one are equal to the initial value of X_{y1}.

3.2.3.6 Training Cost

This provision requires owner/operators to provide all employees and contractors with access to the owner/operator's IT or OT systems basic cybersecurity training that includes cybersecurity awareness to address cyber-hygiene best practices, acceptable use, risks associated with their level of privileged access, and awareness of security risks associated with their actions. The owner/operator must also provide additional role-based training to cybersecurity-sensitive employees. The cost of this provision relates to four areas, including each entity's time burden to develop and implement its cybersecurity training plans, time burdens to all employees to take basic user training, time burdens to privileged users to take role-based training, and recordkeeping.

Each owner/operator must develop, submit, and implement their cybersecurity training plans. TSA estimates PTPR entities would spend 80 hours in Year 1 to develop and implement their

cybersecurity training plans.[281] TSA estimates that this task would be performed by a PTPR COM using a fully-loaded wage rate of $105.82 per hour.

TSA multiplies the same wage rate by the submission hour burden (80 hours) and the entity population to generate a cybersecurity training plan development cost as shown in Table 3-38 below.

Table 3-38: Cybersecurity Training Plan Costs - PTPR ($ Thousands)

Year	PTPR Initial Submissions	PTPR Total Training Plan Cost
	a = Column e, Table 2-1	b = a × 80 hours × $105.82
1	34.00	$287.8
2	0.74	$6.3
3	0.77	$6.5
4	0.77	$6.5
5	0.80	$6.8
6	0.81	$6.9
7	0.83	$7.0
8	0.85	$7.2
9	0.86	$7.3
10	0.89	$7.5
Total		**$349.8**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed. Formulas with X_{yn-1} in year one are equal to the initial value of X_{y1}.

Basic User Awareness Training is intended to provide effective cybersecurity awareness training that helps employees understand proper cyber-hygiene, and the security risks associated with their actions. TSA SMEs with cybersecurity expertise estimate each employee would spend one hour per year completing this training. TSA estimates that 100 percent of the affected freight rail employee population will require basic user training, while 15 percent will require role-based training. TSA calculates basic user awareness training by multiplying the PTPR employee population, by the one hour training burden, and a fully-loaded general PTPR wage rate of

[281] See "Security Training Programs for Surface Transportation Employees – Final Rulemaking." RIN: 1652-AA55. Regulatory Impact Analysis. Page 57. TSA expects the burden hours for the initial submission of the Cybersecurity training plan to be comparable to the burden hours from the Physical Security rulemaking due to the similar length and breadth of requirements, as well as that entities may not yet have experience producing such plans.

$31.23 per hour as described in Section 2.3.2.

Role-based training would consider the role of the privileged user in a cyber-incident as such users bring a unique level of risk to an organization. A privileged user is one that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform. TSA SMEs with cybersecurity expertise estimate the privileged user population as 15 percent of the general user population and estimates privileged users would spend two hours per year completing this training. TSA calculates role-based training costs by multiplying the PTPR privileged user population, by the two hour training burden, and the fully-loaded wage rate of $71.26 per hour described in Section 2.3.2.

Finally, each owner/operator would be required to retain records of initial and recurrent cybersecurity training for everyone required to receive such training. TSA estimates owner/operators would spend 0.02 hours per record handling records, for both basic user awareness training records and role-based training records.[282] TSA calculates training recordkeeping costs by multiplying the number of trainings per year by the 0.02 hour training recordkeeping burden, and the fully loaded administrative assistant's wage rate of $30.07 per hour described in Section 2.3.2.

Table 3-39 presents cybersecurity training costs for PTPR over 10 years. It includes general training, role-based training, and recordkeeping costs.

[282] TSA assumes an administrative assistant for each owner/operator would file a record of each employee's training session. TSA estimates a duration of one-minute (~0.02 hours) for an administrative staff person to file a training record.

Table 3-39: Cybersecurity Training Costs for PTPR ($ Thousands)

Year	PTPR Affected Training Population	General Training Cost	Role-Based Training Cost	Training Recordkeeping Cost	Total Cybersecurity Training Cost
	a = Column d, Table 2-2	b = a × 1 hour × $31.23	c = a × 15% × 2 hours × $71.26	d = (a + (a × 15%)) × (0.02) hours × $30.07	e = b + c + d
1	299,680.00	$9,359.0	$6,406.6	$207.3	$15,972.8
2	303,006.45	$9,462.9	$6,477.7	$209.6	$16,150.1
3	306,369.82	$9,567.9	$6,549.6	$211.9	$16,329.4
4	309,770.52	$9,674.1	$6,622.3	$214.2	$16,510.6
5	313,208.98	$9,781.5	$6,695.8	$216.6	$16,693.9
6	316,685.60	$9,890.1	$6,770.1	$219.0	$16,879.2
7	320,200.81	$9,999.9	$6,845.3	$221.5	$17,066.6
8	323,755.04	$10,110.9	$6,921.2	$223.9	$17,256.0
9	327,348.72	$10,223.1	$6,998.1	$226.4	$17,447.6
10	330,982.29	$10,336.6	$7,075.7	$228.9	$17,641.2
Total		**$98,406.0**	**$67,362.3**	**$2,179.3**	**$167,947.5**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed. Formulas with X_{yn-1} in year one are equal to the initial value of X_{y1}

3.2.3.7 Detection of Cybersecurity Incidents Cost

Under the proposed rule, owner/operators must incorporate into their COIP policies, procedures, and capabilities sufficient to detect and respond to cybersecurity threats, and anomalies on Critical Cyber Systems. These policies, procedures, and capabilities must defend against malicious email, block ingress and egress communications, control the impact of known or suspected malicious web domains or applications, block and defend against unauthorized code or malicious command and control servers, and ensure continuous collection and analysis of data for potential intrusions and anomalous behavior. TSA estimates each affected entity would spend 106.5 hours in Year 1 and 100.5 hours in Years 2 through 10 performing these tasks.[283] In Year 1, this includes four hours to design continuous monitoring criteria, eight hours to develop solutions for IT, two hours per quarter for four network/systems administrators to meet to review

[283] TSA consulted SMEs with cybersecurity expertise and determined that an hour burden range of 106.5 – 211 hours for Year 1 and a range of 100.5 – 197 hours for Years 2-10. TSA uses the lower range estimates as it believes average costs would be closer to the lower values.

security threats (for a total of 32 hours per year), and 15 minutes per work day for updates to the list of blocked websites (a total of 62.5 hours per year).[284] For Years 2 through 10, TSA estimates there will be efficiency gains from experience implementing these process. In Years 2 through 10 TSA estimates each affected entity would spend two hours to design the criteria, four hours to develop solutions for IT, and the continuation of the quarterly meetings and daily updates for an annual burden of 100.50 hours. TSA assumes these tasks would be performed by the COM and network/systems administrator.

TSA calculates a weighted average compensation rate of $68.38 per hour in Year 1 using the fully-loaded wage rate for a COM of $105.82 and for a network/systems administrator of $63.63 per hour.[285] TSA calculates a weighted average compensation rate of $66.15 in Years 2 through 10 due to lower participation of the COM in the time burden.[286]

TSA also estimates an annual cost of $2,995 per owner/operator for the software necessary for continuous monitoring as discussed in Section 2.4.4.8.

Table 3-40 presents continuous monitoring PTPR costs over 10 years. It includes new entity monitoring costs, existing entity monitoring costs, and software costs.

[284] TSA calculates the estimated time burden as 4 hours + 8 hours + (2 hours × 4 quarters × 4 network/systems administrators) + (15 minutes per day × 250 working days per year) ÷ 60 minutes = 62.5 hours) = 106.5 hours in Year 1.
[285] TSA calculates the weighted compensation rate as ($105.82 × 12 hours) + ($63.63 × 94.5 hours) ÷ 106.50 hours. Value used in analysis is rounded to two decimal places.
[286] TSA calculates the weighted compensation rate as ($105.82 × 6 hours) + ($63.63 × 94.5 hours) ÷ 100.50 hours. Value used in analysis is rounded to two decimal places.

Table 3-40: Continuous Monitoring Cost for PTPR ($ Thousands)

Year	New PTPR Affected Entities	Existing PTPR Affected Population	New Entity Cost	Existing Entity Cost	Continuous Monitoring Software Cost	Total PTPR Continuous Monitoring Cost
	a = Column e, Table 2-1	$b_{y1} = 0$ $b_{Yn} = a_{Yn-1} + b_{Yn-1}$	c = a × 106.5 hours × $68.38	d = b × 100.5 hours × $66.15	e = (a + b) × $2,995	f = c + d + e
1	34.00	0.00	$247.6	$0.0	$101.8	$349.4
2	0.74	34.00	$5.4	$226.0	$104.0	$335.5
3	0.77	34.74	$5.6	$231.0	$106.4	$342.9
4	0.77	35.51	$5.6	$236.1	$108.7	$350.3
5	0.80	36.28	$5.8	$241.2	$111.1	$358.1
6	0.81	37.08	$5.9	$246.5	$113.5	$365.9
7	0.83	37.89	$6.0	$251.9	$116.0	$373.9
8	0.85	38.72	$6.2	$257.4	$118.5	$382.1
9	0.86	39.57	$6.3	$263.1	$121.1	$390.4
10	0.89	40.43	$6.5	$268.8	$123.8	$399.0
Total			**$300.9**	**$2,221.9**	**$1,124.7**	**$3,647.6**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed. Formulas with X_{yn-1} in year one are equal to the initial value of X_{y1}.

3.2.3.8 Capabilities to Respond to a Cybersecurity Incident

This provision details additional requirements that owner/operators must include in their COIP capabilities when it comes to responding to cybersecurity incidents that affect Critical Cyber Systems. These specifics are discussed in Section 2.4.4.6 and the time necessary to address these requirements is incorporated into the overall plan development estimates, which is accounted for and discussed in Section 3.2.4.

3.2.3.9 Plan of Action and Milestones (POAM) Cost

Owner/operators who are unable to meet every requirement and security outcome required by the COIP must create a POAM that includes policies, procedures, measures, or capabilities that the owner/operator will develop to ensure all requirements are met. Due to the constantly changing cybersecurity environment, TSA expects a portion of owner/operators would be unable to meet every requirement and security outcome each year and would be required to complete a POAM. As a result of existing voluntary frameworks and compliance with the SDs, TSA estimates 20 percent of owner/operators would need to complete a POAM in the first three years of the rule

and that it will take 80 hours to complete (see Section 2.4.11). TSA invites comment on the proportion of owner/operators who will need to complete a POAM. A TSA SME with cybersecurity expertise estimates a network/systems administrator would spend 48 hours on this task while a cybersecurity analyst will spend 32 hours. TSA calculates a weighted average compensation rate of $63.44 per hour using the fully-loaded wage rate for a network/systems administrator of $63.63 and of $63.16 per hour for the cybersecurity analyst.[287] TSA multiplies the average compensation rate by the POAM hour burden (80 hours) and the affected pipeline entity population to yield the 10-year POAM cost, as shown in Table 3-41 below.

Table 3-41: POAM Cost for PTPR ($ Thousands)

Year	PTPR Affected Population	PTPR Population	Total POAM Cost for PTPR
	a = Column d, Table 2-1	b = {a × 20%, 0}	c = b × 80 hours × $63.44
1	34.00	6.80	$34.5
2	34.74	6.95	$35.3
3	35.51	7.10	$36.0
4	36.28	0	$0.0
5	37.08	0	$0.0
6	37.89	0	$0.0
7	38.72	0	$0.0
8	39.57	0	$0.0
9	40.43	0	$0.0
10	41.32	0	$0.0
Total			**$105.8**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed. Formulas with X_{yn-1} in year one are equal to the initial value of X_{y1}.

3.2.3.10 Total Cost of the COIP

TSA estimates the total cost impact of all COIP components for PTPR entities as $1.2 billion undiscounted over 10 years as presented in Table 3-42 below. The table also presents the total cost of each provision as a percent of total COIP costs. The cost of MFA implementation represents the largest share of PTPR COIP costs at 56.7 percent, largely in part because this cost recurs daily and is driven by employee population.

[287] TSA calculates the weighted compensation rate as ($63.63 × 48 hours) + ($63.15 × 32 hours) ÷ 80 hours. Value used in analysis is rounded to two decimal places.

Table 3-42: Total COIP Cost for PTPR ($ Thousands)

Year	COIP Development and Accountable Executive Designation	Cybersecurity Coordinator Designation	Identification of Critical Cyber Systems	Supply Chain Risk Management	Network Segmentation	Access Control			Patching	Critical System Data Backups	Cyber-security Training	Detection of Cyber-security Incidents	POAM	Total Cost of the COIP for PTPR
						Compliance	MFA Equipment	MFA Implementation						
	Table 3-29	Table 3-30	Table 3-31	Table 3-34	Table 3-33	Table 3-34	Column b, Table 3-35	Column c, Table 3-35	Table 3-38	Table 3-37	Table 3-38 + Table 3-39	Table 3-40	Table 3-41	
1	$129.9	$12.1	$460.1	$944.7	$2,258.6	$311.7	$21,577.0	$67,104.1	$3,428.3	$5,621.7	$16,260.7	$349.4	$34.5	$118,492.8
2	$44.4	$1.9	$125.0	$965.3	$1,732.2	$168.7	$21,816.5	$67,848.9	$3,495.7	$5,875.5	$16,156.4	$335.5	$35.3	$118,601.2
3	$45.4	$1.9	$128.0	$986.7	$1,770.8	$172.5	$22,058.6	$68,602.1	$3,573.2	$6,143.2	$16,335.9	$342.9	$36.0	$120,197.1
4	$46.4	$2.0	$130.6	$1,008.1	$1,808.9	$176.1	$22,303.5	$69,363.5	$3,650.6	$6,420.1	$16,517.2	$350.3	$0.0	$121,777.2
5	$47.4	$2.0	$133.6	$1,030.3	$1,849.0	$180.1	$22,551.0	$70,133.5	$3,731.1	$6,711.9	$16,700.7	$358.1	$0.0	$123,428.7
6	$48.4	$2.0	$136.4	$1,052.8	$1,889.3	$184.0	$22,801.4	$70,912.0	$3,812.6	$7,015.5	$16,886.1	$365.9	$0.0	$125,106.4
7	$49.5	$2.1	$139.4	$1,075.9	$1,930.7	$188.0	$23,054.5	$71,699.1	$3,896.2	$7,333.4	$17,073.6	$373.9	$0.0	$126,816.2
8	$50.6	$2.1	$142.5	$1,099.5	$1,973.1	$192.1	$23,310.4	$72,494.9	$3,981.7	$7,666.0	$17,263.2	$382.1	$0.0	$128,558.3
9	$51.7	$2.2	$145.5	$1,123.4	$2,015.8	$196.3	$23,569.1	$73,299.6	$4,068.2	$8,012.0	$17,454.8	$390.4	$0.0	$130,329.1
10	$52.8	$2.2	$148.8	$1,148.1	$2,060.4	$200.7	$23,830.7	$74,113.3	$4,157.8	$8,376.0	$17,648.8	$399.0	$0.0	$132,138.6
Total	**$566.6**	**$30.6**	**$1,689.9**	**$10,434.8**	**$19,288.7**	**$1,970.1**	**$226,872.6**	**$705,570.9**	**$37,795.4**	**$69,175.4**	**$168,297.3**	**$3,647.6**	**$105.8**	**$1,245,445.7**
% of Total	0.0%	0.0%	0.1%	0.8%	1.5%	0.2%	18.2%	56.7%	3.0%	5.6%	13.5%	0.3%	0.0%	100.0%

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

3.2.4 Reporting Cybersecurity Incidents Cost

Under the proposed rule, owner/operators would be required to report any cybersecurity incident, as defined in the TSA Cybersecurity Lexicon, CISA as soon as practicable, but no later than 24 hours after a cybersecurity incident is identified. The reporting entity must include the contact information of the reporting individual, the affected systems, a description of the incident and threat, earliest known date of compromise, date of detection and other relevant information. TSA utilizes internal data relating to reportable incidents to estimate 0.44 expected PTPR cybersecurity incidents requiring reporting a year per owner/operator as discussed in Section 2.4.10. TSA estimates that each affected entity would incur a one hour time burden to report each incident.[288] A TSA SME with cybersecurity expertise estimates the one hour time burden would be split equally between a cybersecurity analyst and a COM.

TSA calculates a weighted average compensation rate of $84.49 per hour using a fully-loaded wage rate for a cybersecurity analyst of $63.15 and for a COM of $105.82 per hour from Section 2.3.2.[289] TSA then multiplies the weighted average compensation rate ($84.49) by the incident reporting hour burden (1 hour) number of PTPRs per year, and expected incident reporting volume to calculate a freight rail cybersecurity incident reporting costs.

Table 3-43 presents the total PTPR cybersecurity incident reporting cost over 10 years.

[288] This is consistent with the value in ICR 1652-0051 (Rail Security), which estimated 1 hour to report "significant security concerns."

[289] TSA calculates the weighted compensation rate as ($105.82 × 0.5 hours) + ($63.15 × 0.5 hours). Value used in analysis is rounded to two decimal places.

Table 3-43: Cybersecurity Incident Reporting Cost for PTPR ($ Thousands)

Year	PTPR Affected Population	Number of Cybersecurity Incidents	Cost to Report Incidents
	a = Column d, Table 2-1	b = a × 0.44	c = b × 1 hour × $84.49
1	34.00	14.96	$1.3
2	34.74	15.29	$1.3
3	35.51	15.62	$1.3
4	36.28	15.96	$1.3
5	37.08	16.32	$1.4
6	37.89	16.67	$1.4
7	38.72	17.04	$1.4
8	39.57	17.41	$1.5
9	40.43	17.79	$1.5
10	41.32	18.18	$1.5
Total			**$14.0**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

3.2.5 Cybersecurity Incident Response Plan (CIRP) Cost

Under the proposed rule, each affected owner/operator must develop and maintain a CIRP to be filed with TSA. The CIRP must provide specific measures to ensure prompt isolation and segregation of the infected system from the uninfected systems, address the security and integrity of backed-up data, establish capability and governance for implementing mitigation measures, identify which individual is responsible for implementing the CIRP, and conduct exercises to test the plan's effectiveness. TSA estimates that the COM of each affected owner/operator would spend 80 hours in Year 1 to develop the plan and 20 hours in each subsequent year to maintain the plan.

TSA multiplies the COM fully-loaded wage rate of $105.82 discussed in Section 2.3.2 by CIRP development time burden (80 hours) and number of new PTPR entities to estimate CIRP development costs. TSA multiplies the same wage rate by the CIRP maintenance hour burden (20 hours) and number of existing PTPRs to calculate CIRP maintenance costs. Table 3-44 presents PTPR CIRP costs over 10 years. It includes initial CIRP development costs and CIRP annual maintenance costs.

In addition, TSA estimates owner/operators would spend an average of 120 hours to test the

effectiveness of their CIRP. TSA assumes this testing would be completed by the equivalent of a COM. TSA multiplies the fully loaded COM wage rate of $105.82 per hour from Section 2.3.2, CIRP effectiveness testing hour burden (120 hours), and number of PTPR owner/operators to calculate CIRP effectiveness testing costs per year.

Table 3-44: Cybersecurity Incident Response Plan (CIRP) Costs for PTPR ($ Thousands)

Year	New PTPR Affected Entities	Existing PTPR Affected Population	New Entity CIRP Cost	Existing Entity CIRP Cost	CIRP Effectiveness Testing Cost	Total Cost
	a = Column e, Table 2-1	$b_{y1} = 0$ $b_{Yn} = a_{Yn-1} + b_{Yn-1}$	c = a × 80 hours × $105.82	d = b × 20 hours × $105.82	e = (a + b) × 120 hours × $105.82	f = c + d + e
1	34.00	0.00	$287.8	$0.0	$431.7	$719.6
2	0.74	34.00	$6.3	$72.0	$441.1	$519.4
3	0.77	34.74	$6.5	$73.5	$450.9	$531.0
4	0.77	35.51	$6.5	$75.2	$460.7	$542.4
5	0.80	36.28	$6.8	$76.8	$470.9	$554.4
6	0.81	37.08	$6.9	$78.5	$481.1	$566.5
7	0.83	37.89	$7.0	$80.2	$491.7	$578.9
8	0.85	38.72	$7.2	$81.9	$502.5	$591.6
9	0.86	39.57	$7.3	$83.7	$513.4	$604.4
10	0.89	40.43	$7.5	$85.6	$524.7	$617.8
Total			**$349.8**	**$707.3**	**$4,768.8**	**$5,825.9**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed. Formulas with X_{yn-1} in year one are equal to the initial value of X_{y1}.

In addition, each entity would implement its CIRP following a cyber-incident. TSA estimates each entity would spend 160 hours per incident to implement its CIRP as discussed in Section 2.4.6. TSA estimates 60 percent of the hour burden would be performed by a network/systems administrator and 40 percent of the hour burden would be performed by a cybersecurity analyst.[290] TSA calculates a weighted average compensation rate of $63.44 per hour using a fully-loaded wage for a cybersecurity analyst of $63.15 per hour and for a network/systems

[290] TSA SMEs with cybersecurity expertise estimate the estimated time burdens as (160 hours × 0.60 = 96 hours) and (160 hours × 0.40 = 64 hours).

administrator of $63.63 per hour as discussed in Section 2.3.2.[291] TSA multiplies the weighted average compensation rate ($63.44) by the CIRP implementation hour burden (160 hours) and the number of PTPR cybersecurity incidents per year to calculate PTPR CIRP costs as shown in Table 3-45.

Table 3-45: CIRP Implementation Cost for PTPR ($ Thousands)

Year	PTPR Affected Population	Number of Cybersecurity Incidents	Cost to Respond to Incidents
	a = Column d, Table 2-1	b = a × 0.44	c = b × 160 hours × $63.44
1	34.00	14.96	$151.8
2	34.74	15.29	$155.2
3	35.51	15.62	$158.6
4	36.28	15.96	$162.0
5	37.08	16.32	$165.6
6	37.89	16.67	$169.2
7	38.72	17.04	$172.9
8	39.57	17.41	$176.7
9	40.43	17.79	$180.6
10	41.32	18.18	$184.5
Total			$1,677.2

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

3.2.6 Cybersecurity Assessment Plan (CAP) Cost

Under the proposed rule, each owner/operator must develop and maintain a Cybersecurity Assessment Plan (CAP) to be filed with an approved by TSA. The CAP must proactively assess the effectiveness of the COIP, and identify and resolve vulnerabilities associated with identified Critical Cyber Systems, including device, network, or other identified vulnerabilities. TSA estimates that the equivalent of a cybersecurity analyst would spend 40 hours to develop the CAP and a COM and network/systems administrator will each spend two hours reviewing the CAP.[292]

TSA calculates a weighted average compensation rate of $65.11 per hour using the fully-loaded

[291] TSA calculates the weighted compensation rate as ($63.15 × 96 hours) + ($63.63 × 64 hours) ÷ 160 hours. Value used in analysis is rounded to two decimal places.

[292] TSA SMEs with cybersecurity expertise estimate the estimated time burden as 10 hours for the cybersecurity analyst + (2 hours × 2 cybersecurity coordinators = 4 hours) = 14 total hours.

wage rate for a COM of $105.82, for a cybersecurity analyst of $63.15, and a network/systems administrator of $63.63 per hour as discussed in Section 2.3.2.[293] TSA multiplies the average compensation rate by the CAP creation hour burden (44 hours) and the PTPR entity population as shown in Table 3-46 below.

In addition, each entity would implement its CAP by conducting architectural design review (ADR) and penetration testing every two years, beginning in Year 2. While penetration testing is not a stated rule requirement, TSA is including representative costs to reflect actions that may be taken by companies as a part of their processes to be in full compliance with the provisions of the proposed rule in pursuit of a strong CRM program. TSA estimates each entity would conduct penetration testing upon its second full year in the population. TSA estimates each entity would spend 40 hours to conduct the ADR and implement the CAP, with 24 hours attributed to the network/systems administrator and 16 hours attributed to the cybersecurity analyst as discussed in Section 2.4.7. TSA estimates that in addition to the ADR time burden, each entity would incur a flat cost of $20,000 every two years to conduct penetration testing (see Section 2.4.7). [294] TSA estimates each entity would only conduct ADR and penetration testing every 2 years. TSA assumes existing entities would conduct such activities in the second full year after the implementation of the rule. In years between these periods, no existing entities would conduct activities.

TSA calculates a weighted average compensation rate of $63.44 per hour using the fully-loaded

[293] TSA calculates the weighted compensation rate as ($63.15 × 10 hours) + ($105.82 × 2 hours) + ($63.63 × 2 hours) ÷ 14 hours. Value used in analysis is rounded to two decimal places.
[294] RSI Security. What Is The Average Cost Of Penetration Testing?. May 5, 2023, available at https://blog.rsisecurity.com/what-is-the-average-cost-of-penetration-testing/. Accessed September 25, 2023.

wage rate for a cybersecurity analyst of $63.15 and for a network/systems administrator of $63.63 per hour as discussed in Section 2.3.2. [295]

TSA calculates the cost of ADR using the previously described compensation rate multiplied by the ADR hour burden (40 hours) and ADR two-year cycle. TSA similarly estimates penetration testing by multiplying the two-year cycle by the cost of penetration testing ($20,000). Table 3-46 below presents PTPR CAP costs over 10 years.

[295] TSA calculates the weighted compensation rate as ($63.15 × 8 hours) + ($63.63 × 12 hours) ÷ 20 hours. Value used in analysis is rounded to two decimal places.

Table 3-46: Cybersecurity Assessment Plan (CAP) Implementation Cost for PTPR ($ Thousands)

Year	PTPR Affected Population	Initial Population for Penetration Testing	Annual New Entity Growth	New Entities Conducting Penetration Testing	Total Entities Conducting Penetration Tests	Cost to Develop CAP	Cost of Penetration Testing	Total Cost
	a = Column d, Table 2-1	b = {0, a_{y1}}	c = a_{yn} - a_{yn-1}	d = c_{n-1} + d_{n-2}	e = b + d	f = a × 44 hours × $65.11	g = (e × 40 hours × $63.44) + (e × $20,000)	h = f + g
1	34.00	0.00			0.00	$97.4	$0.0	$97.4
2	34.74	34.00	0.74	0.00	34.00	$99.5	$766.3	$865.8
3	35.51	0.00	0.77	0.74	0.74	$101.7	$16.7	$118.4
4	36.28	34.00	0.77	0.77	34.77	$103.9	$783.6	$887.6
5	37.08	0.00	0.80	1.51	1.51	$106.2	$34.0	$140.3
6	37.89	34.00	0.81	1.57	35.57	$108.5	$801.7	$910.2
7	38.72	0.00	0.83	2.32	2.32	$110.9	$52.3	$163.2
8	39.57	34.00	0.85	2.40	36.40	$113.4	$820.4	$933.7
9	40.43	0.00	0.86	3.17	3.17	$115.8	$71.4	$187.3
10	41.32	34.00	0.89	3.26	37.26	$118.4	$839.8	$958.1
Total						**$1,075.9**	**$4,186.1**	**$5,262.0**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed. Formulas with X_{yn-1} in year one are equal to the initial value of X_{y1}.

The CAP must also include a schedule to ensure completion of planned assessments. The schedule must ensure at least 30 percent of the policies, procedures, measures, and capabilities in the COIP are assessed each year and 100 percent are assessed every three years. TSA SMEs with cybersecurity expertise estimate that each owner/operator would incur a time burden of 30 hours annually, or 90 hours over three years, to test the COIP. TSA also estimates a network/systems administrator would incur 18 hours of this time, while a cybersecurity analyst would incur the remaining 12 hours. In addition to this time burden, TSA estimates that each entity would incur a flat cost of $6,667 annually, or $20,000 over three years, to test the COIP as discussed in Section 2.4.7.

TSA calculates a weighted average compensation rate of $63.44 per hour using the fully-loaded wage rate for a cybersecurity analyst of $63.15 and for a network/systems administrator of $63.63 per hour as discussed in Section 2.3.2.[296]

TSA multiplies this compensation rate by COIP testing hour burden (30 hours) and the PTPR entity population to calculate COIP administrative costs. TSA then multiplies COIP testing ($6,667) by the PTPR entity population. Table 3-47 below shows the total PTPR COIP testing costs over 10 years.

[296] TSA calculates the weighted compensation rate as ($63.15 × 2.67 hours) + ($63.63 × 4 hours) ÷ 6.67 hours. Value used in analysis is rounded to two decimal places.

Table 3-47: COIP Testing Cost for PTPR ($ Thousands)

Year	PTPR Population	Administrative Cost	Cost of Testing	Total Cost of COIP Testing
	a = Column d, Table 2-1	b = a × 30 hour × $63.44	c = a × $6,667	d = b + c
1	34.00	$64.7	$226.7	$291.4
2	34.74	$66.1	$231.6	$297.7
3	35.51	$67.6	$236.7	$304.3
4	36.28	$69.0	$241.9	$310.
5	37.08	$70.6	$247.2	$317.8
6	37.89	$72.1	$252.6	$324.7
7	38.72	$73.7	$258.1	$331.8
8	39.57	$75.3	$263.8	$339.1
9	40.43	$76.9	$269.5	$346.5
10	41.32	$78.6	$275.5	$354.1
Total		**$714.7**	**$2,503.6**	**$3,218.3**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

3.2.7 Documentation to Establish Compliance Cost

Each owner/operator would incur various recordkeeping costs, including retaining documents that would be created as part of the CRM process as well as accessing and making these documents available to TSA, as requested. A TSA SME with cybersecurity expertise estimates each affected entity will spend two hours of administrative assistant time annually to meet these obligations. TSA multiplies an administrative assistant fully-loaded wage rate of $30.07 as discussed in Section 2.3.2 by the recordkeeping hour burden (2 hours) and the PTPR entity population to calculate a recordkeeping cost, as shown in Table 3-48 below.

While some of the necessary compliance parameters would be covered under specific rule provisions as part of efforts to comply with the requirements of this proposed rule, TSA additionally estimates an audit manager will incur 40 hours of time to ensure overall compliance with the full rule each year. TSA multiplies an audit manager fully-loaded wage rate of $60.44 as discussed in Section 2.3.2 by the compliance hour burden (40 hours) and the PTPR entity population to calculate a compliance cost, as shown in Table 3-48, below.

Table 3-48: Recordkeeping and Compliance Cost for PTPR ($ Thousands)

Year	PTPR Affected Population	CRM Recordkeeping (Administrative Assistant)	CRM Compliance (Audit Manager)	Total PTPR Recordkeeping Cost
	a = Column d, Table 2-1	b = a × 2 hours × $30.07	c = a × 40 hours × $60.44	d = b + c
1	34.00	$2.0	$82.2	$84.2
2	34.74	$2.1	$84.0	$86.1
3	35.51	$2.1	$85.8	$88.0
4	36.28	$2.2	$87.7	$89.9
5	37.08	$2.2	$89.6	$91.9
6	37.89	$2.3	$91.6	$93.9
7	38.72	$2.3	$93.6	$95.9
8	39.57	$2.4	$95.7	$98.0
9	40.43	$2.4	$97.7	$100.2
10	41.32	$2.5	$99.9	$102.4
Total		**$22.6**	**$907.9**	**$930.5**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

3.2.8 Total Cost Impact to Passenger Railroads and Transit Rail

TSA estimates the total cost impact of all proposed rule requirements for PTPR entities as $1,263.6 million undiscounted over 10 years, $1,074.5 million discounted at 3 percent, and $881.1 million discounted at 7 percent. Table 3-49 shows the total cost of the CRM program, which includes costs related to the CSE, COIP, CAP, Recordkeeping, and Compliance. In Table 3-50 TSA aggregates the various proposed rule costs cost discussed above including Familiarization; the CRM Program; Incident Reporting; and the CIRP. Table 3-50 also presents the percent of total cost for PTPR of each cost category.

Table 3-49: Summary of CRM Program Costs - PTPR ($ Thousands)

Year	CSE	COIP	CAP	Recordkeeping and Compliance	Total Cost of CRM for PTPR
	a = Table 3-27	b = Table 3-42	c = Table 3-46 + Table 3-47	d = Table 3-48	e = ∑a,b,c,d
1	$103.3	$118,492.8	$388.8	$84.2	$119,069.1
2	$105.5	$118,601.2	$1,163.5	$86.1	$119,956.3
3	$107.9	$120,197.1	$422.7	$88.0	$120,815.7
4	$110.2	$121,777.2	$1,198.5	$89.9	$123,175.8
5	$112.7	$123,428.7	$458.0	$91.9	$124,091.3
6	$115.1	$125,106.4	$1,234.9	$93.9	$126,550.3
7	$117.6	$126,816.2	$495.0	$95.9	$127,524.8
8	$120.2	$128,558.3	$1,272.8	$98.0	$130,049.4
9	$122.8	$130,329.1	$533.7	$100.2	$131,085.9
10	$125.5	$132,138.6	$1,312.2	$102.4	$133,678.7
Total	**$1,140.9**	**$1,245,445.7**	**$8,480.3**	**$930.5**	**$1,255,997.4**

Note: Total may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

Table 3-50: Requirement Costs - PTPR ($ Thousands)

Year	Familiarization	CRM Program				Recordkeeping Cybersecurity Incidents	CIRP	Total Cost		
		CSE	COIP	CAP	Recordkeeping and Compliance			h = ∑a,b,c,d,e,f, g		
	a	b	c	d	e	f	g	Undiscounted	Discounted at 3%	Discounted at 7%
1	$54.5	$103.3	$118,492.8	$388.8	$84.2	$1.3	$871.4	$119,996.3	$116,501.3	$112,146.1
2	$1.2	$105.5	$118,601.2	$1,163.5	$86.1	$1.3	$674.5	$120,633.3	$113,708.5	$105,365.8
3	$1.2	$107.9	$120,197.1	$422.7	$88.0	$1.3	$689.6	$121,507.8	$111,196.9	$99,186.6
4	$1.2	$110.2	$121,777.2	$1,198.5	$89.9	$1.3	$704.4	$123,882.8	$110,068.3	$94,509.6
5	$1.3	$112.7	$123,428.7	$458.0	$91.9	$1.4	$720.0	$124,813.9	$107,665.6	$88,990.6
6	$1.3	$115.1	$125,106.4	$1,234.9	$93.9	$1.4	$735.7	$127,288.7	$106,602.3	$84,817.9
7	$1.3	$117.6	$126,816.2	$495.0	$95.9	$1.4	$751.8	$128,279.4	$104,302.9	$79,886.0
8	$1.4	$120.2	$128,558.3	$1,272.8	$98.0	$1.5	$768.3	$130,820.6	$103,271.0	$76,138.8
9	$1.4	$122.8	$130,329.1	$533.7	$100.2	$1.5	$785.0	$131,873.8	$101,070.3	$71,730.6
10	$1.4	$125.5	$132,138.6	$1,312.2	$102.4	$1.5	$802.3	$134,484.0	$100,068.7	$68,364.9
Total	**$66.3**	**$1,140.9**	**$1,245,445.7**	**$8,480.3**	**$930.5**	**$14.0**	**$7,503.1**	**$1,263,580.7**	**$1,074,455.7**	**$881,136.8**
% of Total	0.0%	0.1%	98.6%	0.7%	0.1%	0.0%	0.6%	100.0%		
Annualized									**$125,959.0**	**$125,454.1**

3.3 Cost Impacts to Highway and Motor Carrier Transportation

This section details the costs to Highway and Motor Carrier (OTRB) owner/operators associated with incident reporting as detailed in the proposed rule. Section § 1584 updates the security program requirements covered entities would be required to comply with. This primarily includes the reporting of cybersecurity incidents similar to other transportation modes in this rulemaking. Additional costs related to familiarization are also included below.

3.3.1 Familiarization Cost

TSA anticipates OTRB owner/operators would incur a familiarization cost to review the proposed rule requirements and determine applicability. Familiarization cost includes the time it takes to review the proposed rule's specifications and determine what is needed to achieve compliance. TSA uses a two-pronged approach to estimate familiarization cost. TSA first estimates that each owner/operator across the full industry would review the applicability portion of the rule to determine if they are covered under the scope. According to data from the American Public Transportation Association, there are 1,717 OTRB entities in the industry.[297] TSA expects an individual with the equivalent responsibility of an attorney and an individual with the equivalent responsibility of the accountable executive would each spend a half hour reviewing the applicability portion of the rule, for a total burden of one hour.[298] TSA next calculates a weighted average compensation rate of $103.50 per hour using the fully-loaded wage rate for an attorney of $72.68 and chief executive of $134.31 per hour as discussed in

[297] American Public Transportation Association (APTA). Jan. 2023. 2022 Public Transportation Fact Book. https://www.apta.com/wp-content/uploads/APTA-2022-Public-Transportation-Fact-Book.pdf.

[298] TSA estimates this as a small hour burden based upon the applicability section being short (less than one page) and the reader's inherent knowledge of their company.

Section 2.3.3.[299] TSA then multiplies the weighted average compensation rate ($103.50) by the applicability determination hour burden (1 hour) and number of OTRB entities per year to calculate a total OTRB applicability determination cost.

Next, owner/operators where the rule is applicable would incur costs to review the proposed rule and determine what is needed to achieve compliance. TSA estimates 71 covered owner/operators would review all applicable sections in Year 1 of the proposed rule with new entrants reviewing requirements in subsequent years.[300] TSA estimates an individual with the equivalent responsibility of an accountable executive from each affected owner/operator would spend 1 hour to review the regulation. TSA multiplies a chief executive fully-loaded wage rate of $134.31, as discussed in Section 2.3.3, by the rule review hour burden (1 hours) and number of OTRB entities per year to calculate an OTRB rule review cost.

Table 3-51 presents the total OTRB familiarization cost over 10 years. It includes applicability determination and rule review costs.

[299] TSA calculates the weighted compensation rate as ($72.68 × 0.5 hours) + ($134.31 × 0.5 hours). Value used in analysis is rounded to two decimal places.
[300] See Section 2.1.3 for population information.

Table 3-51: Rule Familiarization Cost for OTRB ($ Thousands)

Year	Total OTRB Affected Population (Growth)	Applicability Determination Cost	Affected OTRB Population (Growth)	Rule Review Cost	Total OTRB Familiarization Cost
	a = (a_{Y1} × (1 + 2.50%) ^ (Y_n – 1)) - ∑($a_{Yn...}$ a_{Yn} – 1)	b = a × 1 hour × $103.50	c = Column h, Table 2-1	d = c × 1 hour × $134.31	e = b + d
1	1717.00	$177.7	71.00	$9.5	$187.2
2	42.93	$4.4	1.78	$0.2	$4.7
3	43.99	$4.6	1.81	$0.2	$4.8
4	45.10	$4.7	1.87	$0.3	$4.9
5	46.23	$4.8	1.91	$0.3	$5.0
6	47.38	$4.9	1.96	$0.3	$5.2
7	48.56	$5.0	2.01	$0.3	$5.3
8	49.78	$5.2	2.06	$0.3	$5.4
9	51.03	$5.3	2.11	$0.3	$5.6
10	52.30	$5.4	2.16	$0.3	$5.7
Total		**$221.9**		**$11.9**	**$233.8**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed. Formulas with X_{yn-1} in year one are equal to the initial value of X_{y1}.

3.3.2 Reporting Cybersecurity Incidents Cost

Under the proposed rule, owner/operators would be required to report any cybersecurity incident, as defined in the TSA Cybersecurity Lexicon, CISA as soon as practicable, but no later than 24 hours after a cybersecurity incident is identified. The reporting entity must include the contact information of the reporting individual, the affected systems, a description of the incident and threat, earliest known date of compromise, date of detection and other relevant information. TSA utilizes internal data relating to reportable incidents to estimate 0.21 expected OTRB cybersecurity incidents requiring reporting a year per owner/operator as discussed in Section 2.4.10. TSA estimates that each affected entity would incur a one hour time burden to report each incident as discussed in Section 2.4.5. TSA expects the one hour time burden would be split equally between an individual with the equivalent responsibility of a cybersecurity analyst and a COM.[301]

[301] The proposed rule does not include a requirement for OTRB owner/operators to have a security coordinator, but TSA assumes someone with a comparable level of understand and wage would perform necessary reporting tasks.

TSA calculates a weighted average compensation rate of $84.49 per hour using a fully-loaded wage rate for a cybersecurity analyst of $63.15 and for a COM of $105.82 per hour, as discussed in Section 2.3.3.[302] TSA then multiplies the weighted average compensation rate ($84.49) by the incident reporting hour burden (1 hour), number of OTRB entities per year, and expected incident reporting volume to calculate a OTRB cybersecurity incident reporting costs.

Table 3-52 presents the total OTRB cybersecurity incident reporting cost over 10 years.

Table 3-52: Cybersecurity Incident Reporting Cost for OTRB ($ Thousands)

Year	Affected OTRB Population (Growth)	Number of Cybersecurity Incidents	Cost to Report Incidents
	a = Column g, Table 2-1	b = a × 0.21	c = b × 1 hour × $84.49
1	71.00	14.91	$1.3
2	72.78	15.28	$1.3
3	74.59	15.66	$1.3
4	76.46	16.06	$1.4
5	78.37	16.46	$1.4
6	80.33	16.87	$1.4
7	82.34	17.29	$1.5
8	84.40	17.72	$1.5
9	86.51	18.17	$1.5
10	88.67	18.62	$1.6
Total			$14.1

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

3.3.3 Total Cost Impact to Highway Motor Carrier Transportation

In Table 3-53, TSA estimates the total cost impact of all proposed rule requirements for OTRB entities, over the ten-year period of analysis, as $247.9 million undiscounted, $232.7 million discounted at 3 percent, and $215.9 million discounted at 7 percent. TSA sums the familiarization (Table 3-51) and incident reporting costs (Table 3-52) for OTRB entities.

[302] TSA calculates the weighted compensation rate as ($105.82 × 0.5 hours) + ($63.15 × 0.5 hours) ÷ 1 hour. Value used in analysis is rounded to two decimal places.

Table 3-53: Summary of Proposed Rule Requirement Costs - OTRB ($ Thousands)

Year	Familiarization	Reporting Cybersecurity Incidents	Total Cost		
			c = a + b		
	a	b	Undiscounted	Discounted at 3%	Discounted at 7%
1	$187.2	$1.3	$188.5	$183.0	$176.2
2	$4.7	$1.3	$6.0	$5.6	$5.2
3	$4.8	$1.3	$6.1	$5.6	$5.0
4	$4.9	$1.4	$6.3	$5.6	$4.8
5	$5.0	$1.4	$6.4	$5.5	$4.6
6	$5.2	$1.4	$6.6	$5.5	$4.4
7	$5.3	$1.5	$6.8	$5.5	$4.2
8	$5.4	$1.5	$6.9	$5.5	$4.0
9	$5.6	$1.5	$7.1	$5.4	$3.9
10	$5.7	$1.6	$7.3	$5.4	$3.7
Total	**$233.8**	**$14.1**	**$247.9**	**$232.7**	**$215.9**

Note: Totals may not add due to rounding.

3.4 Cost Impacts to Pipeline Transportation

This section details the costs to pipeline owner/operators associated with the creation and maintenance of a CRM Program as detailed in the proposed rule. Section § 1586.203 details the components covered entities would be required to have in their CRM programs as well as parameters for subsidiaries. These include a cybersecurity evaluation (CSE), a TSA-approved Cybersecurity Operational Implementation Plan (COIP), and a Cybersecurity Assessment Plan (CAP) whose costs are discussed in Sections 3.4.4 (CSE), 3.4.5 (COIP), and 3.4.8 (CAP), accordingly. Additionally, Sections § 1586.103 and 1586.105 add additional requirements related to the physical security portion of the pipeline security program. These costs are captured in sections 3.4.2 and 3.4.3. Additional costs related to familiarization, reporting cybersecurity incidents, as well as recordkeeping and documentation are also included below. Note that in contrast to freight and passenger railways, TSA does not anticipate a growth rate to affected pipeline entities in this analysis.

3.4.1 Familiarization Cost

TSA anticipates pipeline owner/operators would incur a familiarization cost to review the

proposed rule requirements and determine applicability. Familiarization cost includes the time it takes to review the proposed rule's specifications and determine what is needed to achieve compliance. TSA uses a two-pronged approach to estimate familiarization. TSA first estimates that each owner/operator across the full industry would review the applicability portion of the rule to determine if they are covered under the scope. According to TSA data, there are 2,105 pipeline owner/operators in the industry.[303] TSA expects an attorney and an individual with the equivalent responsibility of the accountable executive would each spend a half hour reviewing the applicability portion of the rule for a total burden of one hour.[304] TSA calculates a weighted average compensation rate of $273.76 per hour using the fully-loaded wage rate for an attorney of $280.21 and accountable executive of $267.30 per hour, as discussed in Section 2.3.4.[305] TSA then multiplies the weighted average compensation rate ($273.76) by the applicability determination hour burden (1 hour) and number of pipelines per year to calculate a total pipeline applicability determination cost.

Second, owner/operators for whom the rule is applicable would incur costs to review the proposed rule and determine what is needed to achieve compliance. TSA assumes that a COM and an attorney within covered owner/operators would review all applicable sections in Year 1 of the proposed rule with new individuals reviewing in subsequent years.[306]

TSA estimates that a COM and an attorney from each affected owner/operator would each spend

---

[303] See Section 2.1.4.
[304] TSA estimates this as a small hour burden based upon the applicability section being short (less than one page) and the reader's inherent knowledge of their company.
[305] TSA calculates the weighted compensation rate as ($280.21 × 0.5 hour) + ($267.30 × 0.5 hour) ÷ 1 hour. Value used in analysis is rounded to two decimal places.
[306] See Section 2.1.4 for estimates on number of small and large entities. TSA assumes this distribution remains constant over the 10-year period of analysis.

7.08 hours to review the regulation, as discussed in Section 2.4.1. TSA additionally estimates that 15 minutes of time will be taken for a COM to brief an accountable executive on the requirements of the rule.

TSA next calculates a weighted average compensation rate of $198.93 per hour in Year 1 using the fully-loaded wage rate for a COM of $118.09, an attorney of $280.21, and accountable executive of $267.30 per hour.[307] TSA then multiplies the weighted average compensation rate by the rule review hour burden (14.66 hours) to calculate a pipeline rule review cost.

Table 3-54 presents the total pipeline familiarization cost over 10 years. It includes applicability determination and rule review costs.

Table 3-54: Pipeline Familiarization Cost ($ Thousands)

Year	Total Pipeline Population	Applicability Determination Cost	Pipeline Affected Population	Rule Review Cost	Total Pipeline Familiarization Cost
	a_{Y1} = 2,105.00	b = a × 1 hour × $273.76	c_{Y1} = 115.00	d = c × 14.66 hours × $198.93	e = b + d
1	2,105.00	$576.3	115.00	$335.4	$911.6
2	-	-	-	-	-
3	-	-	-	-	-
4	-	-	-	-	-
5	-	-	-	-	-
6	-	-	-	-	-
7	-	-	-	-	-
8	-	-	-	-	-
9	-	-	-	-	-
10	-	-	-	-	-
Total		**$576.3**		**$335.4**	**$911.6**

Note: Calculation may not be exact due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

3.4.2 Physical Security Coordinator Cost

This provision requires pipeline owner/operators to provide in writing to TSA the names, titles,

[307] TSA calculates the total time burden as 14.66 = (7.08 hours × 2) + 0.25 hours + 0.25 hours. TSA calculates the weighted compensation rate as (($267.30 × 0.25 hours) + ($118.09 × 7.33 hours) + ($280.21 × 7.08 hours)) ÷ 14.66 hours. Value used in analysis is rounded to two decimal places.

phone number(s), and email address(es) of the physical security coordinator and alternate physical security coordinator(s) within seven days of the commencement of new operations or change in any of the information required by this section. The cost of this requirement is the time each entity takes to designate a physical security coordinator and alternate and to submit that information to TSA. TSA estimates all covered owner/operators would provide this information in Year 1 of the proposed rule; thereafter, covered owner/operators would provide updated information to account for turnover or changes in names, titles, phone number(s), or email address(es) each year. TSA estimates a 14 percent turnover rate as discussed in Section 2.2. TSA estimates an average of 2.27 coordinators would be designated per owner/operator resulting in 261.05 coordinators designated in Year 1. Given employee turnover, TSA estimates that 36 physical security coordinators would be designated in Years 2 through 10. TSA estimates a time burden of 0.5 hours of security manager time per designated physical security coordinator.[308]

TSA assumes an audit manager at a fully-loaded wage rate of $138.10, as discussed in Section 2.3.4, would designate a physical security coordinator. In Table 3-55, TSA calculates the ten-year cost to designate physical security coordinators by multiplying the annual number of designations by the $138.10 audit manager compensation rate and 0.5 hour burden.

[308] Owner/operators would need to provide TSA with the names, titles, and contact information of all appointed security coordinators. Based on input from SMEs in the Surface Division, TSA estimates an industry manager would spend 30 minutes per submission.

Table 3-55: Physical Security Coordinator Designation Cost for Pipeline ($ Thousands)

Year	Pipeline Affected Population	Pipeline New Physical Security Coordinator Population	Pipeline New Physical Security Coordinator Cost
	a_{Y1} = 115.00 a_{yn} = 0	$b_{y1} = a_{y1} \times 2.27$ $b_{yn} = a_{Yn} \times 2.27 + (a_{Y1} \times 2.27 \times 14\%)$	c = b × 0.5 hours × $138.10
1	115.00	261.05	$18.0
2	-	35.69	$2.5
3	-	35.69	$2.5
4	-	35.69	$2.5
5	-	35.69	$2.5
6	-	35.69	$2.5
7	-	35.69	$2.5
8	-	35.69	$2.5
9	-	35.69	$2.5
10	-	35.69	$2.5
Total			**$40.2**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

3.4.3 Reporting Physical Security Incidents Cost

Under the proposed rule, each pipeline entity would be required to report any potential threats and significant physical security concerns involving transportation-related operations to TSA as soon as practicable, but no later than 24 hours after an incident is identified. The reporting entity must include the contact information of the reporting individual, the affected systems, a description of the incident and threat, earliest known date of compromise, date of detection and other relevant information. TSA estimates that 25.29 calls would be made per pipeline entity per year to report such incidents.[309] TSA therefore calculates a total of 2,908.35 incidents reported each year, and estimates a time burden of 0.05 hours per call.[310]

TSA uses a fully-loaded wage rate of $130.24 for a physical security coordinator to make such calls as discussed in Section 2.3.4. TSA then multiplies the same wage rate ($130.24) by the

[309] TSA uses data from its Transportation Security Operations Center, based on 10 months of record, to estimate an expected increase of 101.14 calls per bus-only PTPR owner/operator. However, given uncertainty in the number of pipeline physical security incidents, TSA estimates a reduction to 25 percent of this original value for a total of 25.29 incidents per entity per year.

[310] TSA calculates the total number of incidents as 25.29 × 115 = 2,908. TSA data from the Transportation Security Operations Center (TSOC) shows that the average phone call is approximately 3 minutes (0.05 hours) in duration.

expected number of reportable physical security incidents per year and the incident reporting hour burden (0.05) to calculate a Physical Security Incident reporting cost for pipeline owner/operators. Table 3-56 below shows the ten-year costs for physical security incident reporting.

Table 3-56: Physical Security Incident Reporting Cost for Pipelines ($ Thousands)

Year	Number of Affected Pipeline Entities	Number of Physical Security Incidents	Cost to Report Physical Security Incidents
	a = Column j, Table 2-1	b = a × 25.29	c = b × 0.05 hours × $130.24
1	115.00	2,908.35	$18.9
2	115.00	2,908.35	$18.9
3	115.00	2,908.35	$18.9
4	115.00	2,908.35	$18.9
5	115.00	2,908.35	$18.9
6	115.00	2,908.35	$18.9
7	115.00	2,908.35	$18.9
8	115.00	2,908.35	$18.9
9	115.00	2,908.35	$18.9
10	115.00	2,908.35	$18.9
Total			$189.4

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

3.4.4 Cybersecurity Evaluation (CSE) Cost

The CSE provision requires that each owner/operator required to have a CRM program complete an initial and recurrent cybersecurity evaluation. The cost of this requirement relates to the time burden for entities to conduct the evaluation as well as for any costs incurred to immediately address risks identified. TSA SMEs with cybersecurity expertise first estimate an annual average time to conduct this evaluation of 120 hours, which includes 60 hours of a cybersecurity analyst and 60 hours of a network/systems administrator's time.

TSA next calculates a weighted average compensation rate of $66.11 per hour using the fully-loaded wage rate for a cybersecurity analyst of $71.00 and network/systems administrator of

$61.21 per hour as discussed in Section 2.3.4.[311] TSA then multiplies the weighted average compensation rate ($66.11) by the evaluation hour burden (120 hours) and number of pipelines per year to calculate pipeline evaluation costs per year.

Next, TSA assumes some entities would choose to immediately plan how to address some of the risk areas discovered while others would wait to address risks through their COIP. Surface transportation SMEs estimate that 20 percent of owner/operators would choose to plan to address risks immediately upon completion of their evaluation. TSA assumes that such efforts would occur each year following the evaluation and that a cybersecurity analyst and network/systems administrator would each spend an average of 20 hours planning to address identified risks for a total 40 hours.[312] TSA next calculates a weighted average compensation rate of $66.11 per hour using the fully-loaded wage rate for a cybersecurity analyst of $71.00 and network/systems administrator wage rate of $61.21 per hour.[313] TSA then multiplies the weighted average compensation rate ($66.11) by the evaluation risk reduction hour burden (40 hours), percent of owner/operators who take action (20 percent), and number of pipelines per year to calculate a pipeline evaluation risk reduction cost.

Table 3-57 presents the total pipeline CSE cost over 10 years. It includes cybersecurity evaluation and risk reduction costs.

[311] TSA calculates the weighted compensation rate as ($71.00 × 60 hours) + ($61.21 × 60 hours) ÷ 120 hours. Value used in analysis is rounded to two decimal places.
[312] TSA calculates the estimated time burden as twenty (20) hours for a cybersecurity analyst + twenty (20) hours for network/systems administrator = forty (40) hours total.
[313] TSA calculates the weighted compensation rate as ($71.00 × 20) hours + ($61.21 × 20 hours) ÷ 40 hours. Value used in analysis is rounded to two decimal places.

Table 3-57: Cybersecurity Evaluation (CSE) Cost for Pipeline ($ Thousands)

Year	Pipeline Affected Population	CSE Annual Evaluation Cost	Implementation Population	CSE Implementation Cost	Total CSE Cost
	a = Column j, Table 2-1	b = a × 120 hours × $66.11	c = a × 20%	d = c × 40 hours × $66.11	e = b + d
1	115.00	$912.3	23.00	$60.8	$973.1
2	115.00	$912.3	23.00	$60.8	$973.1
3	115.00	$912.3	23.00	$60.8	$973.1
4	115.00	$912.3	23.00	$60.8	$973.1
5	115.00	$912.3	23.00	$60.8	$973.1
6	115.00	$912.3	23.00	$60.8	$973.1
7	115.00	$912.3	23.00	$60.8	$973.1
8	115.00	$912.3	23.00	$60.8	$973.1
9	115.00	$912.3	23.00	$60.8	$973.1
10	115.00	$912.3	23.00	$60.8	$973.1
Total		**$9,123.2**		**$608.2**	**$9,731.4**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

3.4.5 Cybersecurity Operational Implementation Plan (COIP) Cost

Each owner/operator required to have a CRM program must adopt a Cybersecurity Operational Implementation Plan (COIP). The development and implementation of one's COIP involves a level of governance that includes identifying information about the owner/operator, including an accountable executive responsible for the sustainment of the company's cybersecurity program and providing a written attestation that the plan has been reviewed, and identification of operations which meet the applicability requirements. The COIP also requires owner/operators to address specific content, including the designation of cybersecurity coordinators, identification of Critical Cyber Systems requiring protection, creating policies and procedures to protect Critical Cyber Systems, detect cybersecurity incidents, and respond to detected cybersecurity incidents. The COIP also requires owner/operators to develop and implement cybersecurity training for general and IT specialist populations, develop standards for ensuring supply chain risk management, backup Critical Cyber Systems, and develop capabilities to respond to a cybersecurity incident. Furthermore, to the extent that the owner/operator does not meet the requirements mentioned above such owner/operator must create a plan of action and milestones

(POAM) to achieve those outcomes. The costs associated with these COIP requirements are detailed in subsections below.

3.4.5.1 Governance of the CRM Program

TSA estimates owner/operators would spend 40 hours setting up an initial COIP in Year 1 and providing identifying information as discussed in Section 2.4.4. For years 2-10, TSA assumes owner/operators would spend 40 hours, in any one year in a three-year period, presented as an annual average of 13.33 hours. TSA assumes time spent on this requirement would be evenly split between a COM and a corporate attorney. TSA calculates a weighted average compensation rate of $199.15 per hour using the fully-loaded wage rate for an attorney of $280.21 and of $118.09 per hour for the COM. [314] TSA then multiplies the weighted average compensation rate ($199.15) by the COIP development hour burden (40 hours) and number of affected pipeline entities per year to calculate a pipeline COIP development cost in Year 1. TSA then multiplies the weighted average compensation rate ($199.15) by the subsequent year COIP development burden (13.33 hours) and number of affected pipeline entities per year to calculate a pipeline COIP development cost in Years 2-10.

In addition, owner/operators must identify an accountable executive of the organization responsible for the sustainment of the company's cybersecurity program and have final approval authority over program parameters. The cost of this requirement is the time it takes each affected owner/operator to identify such executive-level individual(s).[315] Given the complexity of CRM

[314] TSA calculates the weighted compensation rate as ($280.21 × 20 hours) + ($118.09 × 20 hours) ÷ 40 hours. Value used in analysis is rounded to two decimal places.

[315] TSA incorporates time for the accountable executive to review the components of the CRM program, including the COIP, CSE, CAP, Cybersecurity Training Plans and CIRP as discussed in the sections below. The accountable executive is allocated 4 hours to review the COIP for compliance and adequacy, 4 hours for training plan review.

programs, TSA recognizes that some entities may require more than one individual to hold this designation but for purposes of this analysis, has assumed that affected owner/operators will select one individual in order to meet the requirements of the rule, as shown in Table 3-58.

Table 3-58: Accountable Executive Population for Pipeline

Year	Pipeline Population	Number of Accountable Executives	Number of New Accountable Executives Resulting From Employee Turnover	Total Number of New Accountable Executives
	a = Column j, Table 2-1	$b_{y1} = a_{y1}$ $b_{yn} = a_{yn} - a_{yn-1}$	$c_{y1} = 0$ $c_{yn} = a_{Yn} \times 13.67\%$	d = b + c
1	115.00	115.00	0.00	115.00
2	115.00	0.00	15.72	15.72
3	115.00	0.00	15.72	15.72
4	115.00	0.00	15.72	15.72
5	115.00	0.00	15.72	15.72
6	115.00	0.00	15.72	15.72
7	115.00	0.00	15.72	15.72
8	115.00	0.00	15.72	15.72
9	115.00	0.00	15.72	15.72
10	115.00	0.00	15.72	15.72
Total		**115**	**141**	**256**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed. Formulas with X_{yn-1} in year one are equal to the initial value of X_{y1}.

TSA estimates that owner/operators would spend three hours making this determination per identified individual, split between one hour of COM time to make the designation and two hours of attorney time to review and document the qualifying criteria for small entities. TSA next calculates a weighted average compensation rate of $226.17 per hour using the fully-loaded wage rate for a COM of $118.09 and an attorney of $280.21 per hour for small entities.[316]

In addition, TSA estimates an accountable executives turnover rate of 14 percent, as discussed in Section 2.2, that would necessitate a new designation. TSA then multiplies the number of accountable executives, the hour burden per accountable executive, and the weighted average

[316] TSA calculates the weighted compensation rate as (($280.21 × 2 hours) + ($118.09 × 1 hours)) ÷ 3 hours. Value used in analysis is rounded to two decimal places.

compensation wage to determine the accountable executive designation cost for entities. The total accountable executive designation cost is presented Table 3-59.

Table 3-59: COIP Governance Cost for Pipelines ($ Thousands)

Year	Pipeline Population	COIP Development	Pipeline Accountable Executive Population	Accountable Executive Designation Cost	Pipeline Total COIP Governance Cost
	a = Column j, Table 2-1	b = a × 13.33 hours × $199.15	c = Table 3-58	d = c x 3 hours x $226.17	e = b + d
1	115.00	$916.1	115.00	$78.0	$994.1
2	115.00	$305.3	15.72	$10.7	$316.0
3	115.00	$305.3	15.72	$10.7	$316.0
4	115.00	$305.3	15.72	$10.7	$316.0
5	115.00	$305.3	15.72	$10.7	$316.0
6	115.00	$305.3	15.72	$10.7	$316.0
7	115.00	$305.3	15.72	$10.7	$316.0
8	115.00	$305.3	15.72	$10.7	$316.0
9	115.00	$305.3	15.72	$10.7	$316.0
10	115.00	$305.3	15.72	$10.7	$316.0
Total		**$3,663.7**		**$174.0**	**$3,837.7**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

3.4.5.2 Cybersecurity Coordinator Cost

This provision requires owner/operators to provide in writing to TSA the names, titles, phone number(s), and email address(es) of the cybersecurity Coordinator and alternate cybersecurity Coordinator(s) within seven days of the commencement of new operations or change in any of the information required by this section. The cost of this requirement is the time each entity takes to designate a cybersecurity coordinator and alternate and to submit that information to TSA. TSA estimates all covered owner/operators will provide this information in Year 1 of the proposed rule; thereafter, covered owner/operators will need to provide updated information to account for turnover or changes in names, titles, phone number(s), or email address(es) each year. TSA estimates a 13.67 percent turnover rate as discussed in Section 2.2.

Each owner/operator vets the qualifications of the cybersecurity coordinator to determine if they meet the requirements of the role. TSA estimates that all entities would have two individuals

filling this role of coordinator and alternate. TSA estimates that a COM will take 15 minutes of time to designate the cybersecurity coordinator, each designated cybersecurity coordinator would take 45 minutes of their time to provide contact details to TSA, and an attorney would spend one hour of time to review, select, and vet the identified individual to ensure the qualifications of the designated individuals. This results in a total of two hours per designation.

TSA next calculates a weighted average compensation rate of $199.15 per hour using the fully-loaded wage rate for a cybersecurity coordinator of $118.09, for a COM of $118.09, and for an attorney of $280.21.[317] TSA multiplies the number of cybersecurity coordinators by the weighted average compensation rate ($199.15) and cybersecurity coordinator designation hour burden (2 hours) to calculate a cybersecurity coordinator designation cost as presented in Table 3-60.

Table 3-60: Cybersecurity Coordinator Cost for Pipeline ($ Thousands)

Year	Pipeline Affected Population	Number of Initial Cybersecurity Coordinators	Number of New Cybersecurity Coordinators Resulting From Employee Turnover	Total Number New of Cybersecurity Coordinators	Pipeline Cybersecurity Coordinator Cost
	a = Column j, Table 2-1	$b_{y1} = a_{y1} \times 2$ $b_{yn} = (a_{yn} - a_{yn-1}) \times 2$	$c_{y1} = 0$ $c_{yn} = a_{yn} \times 2 \times 13.67\%$	d = b + c	e = d × 2 hours × $199.15
1	115.00	230.00	0.00	230.00	$91.6
2	115.00	0.00	31.44	31.44	$12.5
3	115.00	0.00	31.44	31.44	$12.5
4	115.00	0.00	31.44	31.44	$12.5
5	115.00	0.00	31.44	31.44	$12.5
6	115.00	0.00	31.44	31.44	$12.5
7	115.00	0.00	31.44	31.44	$12.5
8	115.00	0.00	31.44	31.44	$12.5
9	115.00	0.00	31.44	31.44	$12.5
10	115.00	0.00	31.44	31.44	$12.5
Total		**230**	**283**	**513**	**$204.3**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.
Formulas with X_{yn-1} in year one are equal to the initial value of X

[317] TSA calculates the weighted compensation rate as ($118.09 × 1 hour) + ($280.21 × 0.25 hours) + ($280.21 × 0.75 hours) ÷ 2 hours. Value used in analysis is rounded to two decimal places.

3.4.5.3 Identification of Critical Cyber Systems Cost

Under the proposed rule, owner/operators must incorporate a list of Critical Cyber Systems, as defined in the TSA Cybersecurity Lexicon, into its COIP that provides, at a minimum an identifier and system specific information, such as the system/manufacturer/designer name for each Critical Cyber System. The owner/operator must also discuss its identification methodology and provide system architecture and connection information. Affected owner/operators would incur costs to design its identification protocol and conduct a review of its inventory to designate Critical cyber Systems, and ensure such systems are defined in the TSA Cybersecurity Lexicon.[318] TSA SME with cybersecurity expertise estimates affected entities would spend an average of 160 hours in Year 1 performing these tasks and 40 hours in subsequent years (Years 2 through 10) to review and update, as discussed in Section 2.4.4.3. In Year 1, these 160 hours include time to design the criteria, conduct an IT and OT inventory, create a database and update it, as well as time to integrate criticality designations. For Years 2 through 10, TSA estimates there will efficiency gains from experience implementing these processes as shown in Table 2-10. These tasks would be performed by the COM, network/systems administrator, and a cybersecurity analyst.

TSA calculates a weighted average compensation rate of $92.59 using a fully-loaded wage rate for a cybersecurity analyst of $71.00, for a network/systems administrator of $61.21, and for a COM of $118.09 per hour.[319]

TSA multiplies the same wage rate multiplied the new entity hour burden to identify Critical

[318] See Section III(F)(2) of the Notice of Proposed Rulemaking for information on TSA's Cybersecurity Lexicon.
[319] TSA calculates the weighted compensation rate as ($118.09 ×40 hours × 50%) + ($61.21 × 160 hours × 30%) + ($71.00 × 160 hours × 20%). Value used in analysis is rounded to two decimal places.

Cyber Systems (160 hours) plus the wage rate for existing entities multiplied by the existing entity hour burden (40 hours) to calculate a Critical Cyber Systems identification cost as presented in Table 3-61.

Table 3-61: Identification of Critical Cyber Systems Cost for Pipeline ($ Thousands)

Year	Pipeline Population	Total Identification of Critical Cyber Systems Cost
	a = Column j, Table 2-1	b = {a_{Y1} × 160 hours × $92.59, a_{Yn} × 40 hours × $92.59}
1	115.00	$1,703.7
2	115.00	$425.9
3	115.00	$425.9
4	115.00	$425.9
5	115.00	$425.9
6	115.00	$425.9
7	115.00	$425.9
8	115.00	$425.9
9	115.00	$425.9
10	115.00	$425.9
Total		**$5,536.9**

Notes: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

3.4.5.4 Supply Chain Risk Management Cost

Under the proposed rule, owner/operators must incorporate into their COIP policies, procedures, and capabilities to address supply chain cybersecurity vulnerabilities. This includes ensuring all procurement documents and contracts include a requirement for the vendor or service provider to notify the owner/operator of cybersecurity incidents, vulnerabilities, and an evaluation of the cybersecurity measures implemented by vendors. In addition, owner/operators must consider the level of cybersecurity sufficient to protect against or respond to cybersecurity incidents and mitigation measures to address risks identified by the vendor or service provider. The cost of this requirement includes the time incurred for contract renewals and updates to come into compliance, as well as the time owner/operators spend to check the goods, services, or capabilities provided by vendors or service providers to identify potential vulnerabilities. TSA estimates affected entities would spend an average of 330 hours annually to perform these

tasks.[320] This includes 10 hours of attorney time to review and update contracts and 40 hours for a team of four individuals to check vendor provided capabilities twice a year. TSA estimates checking vendor provided capabilities would be split between a COM who will incur a time burden of 160 hours, a cybersecurity analyst who will incur 112 hours of time, and a network/systems administrator who will incur 48 hours of time.[321]

TSA calculates a weighted average compensation rate of $98.75 per hour using the fully-loaded wage rate for an attorney of $280.21, a COM of $118.09, a cybersecurity analyst of $71.00, and a network/systems administrator of $61.21 per hour.[322]

TSA then multiplies the weighted average compensation rate ($98.75) by the supply chain risk management hour burden (330 hours) and number of pipelines per year to calculate a pipeline supply chain risk management cost per year as presented in Table 3-62.

Table 3-62: Supply Chain Risk Management Cost for Pipelines ($ Thousands)

Year	Pipeline Population	Total Supply Chain Risk Management Cost for Pipeline
	a = Column j, Table 2-1	b = a × 330 hours × $98.75
1	115.00	$3,747.6
2	115.00	$3,747.6
3	115.00	$3,747.6
4	115.00	$3,747.6
5	115.00	$3,747.6
6	115.00	$3,747.6
7	115.00	$3,747.6
8	115.00	$3,747.6
9	115.00	$3,747.6
10	115.00	$3,747.6
Total		**$37,475.6**

Notes: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

[320] TSA estimates four (4) cybersecurity analysts will spend 40 hours twice a year. 4 analysis × 40 hours × 2 times a year = 320. 320 hours for the cybersecurity analysts + 10 hours for an attorney = 330 hours.

[321] TSA SMEs with cybersecurity expertise estimate the division of the hour burden will consist of 50% Cybersecurity coordinator, 35% cybersecurity analyst, and 15% network/systems administrator.

[322] TSA calculates the weighted compensation rate as (($280.21 × 10 hours) + ($118.09 × 160 hours) + ($71.00 × 112 hours) + ($61.21 × 48 hours)) ÷ 330 hours. Value used in analysis is rounded to two decimal places.

3.4.5.5 Protection of Critical Cyber Systems Cost

Under the proposed rule, owner/operators must incorporate into its COIP network segmentation, procedures, controls and capabilities to protect Critical Cyber Systems that are sufficient to protect against disruption of IT and OT, secure and defend zone boundaries, control access to Critical Cyber Systems to prevent unauthorized access, reduce the risk of exploitation of unpatched systems through the application of security patches and updates, ensure logging data are stored and maintained properly, ensure all Critical Cyber Systems are regularly backed up, and other policies. The cost related to network segmentation involves developing and implementing policies to properly segment OT and IT.

TSA estimates affected entities would spend 820 hours in Year 1 and 660 hours in subsequent years (Years 2 through 10) performing this task.[323] TSA estimates the 820-hour total time burden in Year 1 is comprised of 100 hours to design the criteria, 120 hours to conduct an inventory of OT, 120 hours to review OT to OT connections, 120 hours to review OT to IT connections, 120 hours to review OT connections to third parties and 240 hours to develop networking solutions to ensure OT and IT are separate.

For Years 2 through 10, TSA estimates each of the above tasks will continue each year, TSA estimates components of the time burden relating to the application will remain constant and the time burden to design the segmentation criteria will fall by 40 percent to 60 hours per entity per year.[324] A TSA SME with cybersecurity expertise also estimates the time burden to design

[323] TSA consulted SMEs with cybersecurity expertise and determined that an hour burden range of 320 – 840 hours for Year 1 and a range of 240 – 660 hours for Years 2-10. TSA decided to use an hour burden of 820 hours for Year 1 and 660 hours for Years 2-10 as it determined the upper bound represented the average time it would take for affected owner/operators to complete these tasks.

[324] TSA SMEs with cybersecurity expertise estimate the hour burden for Years 2-10 as 60 + 120 + 120 + 120 + 120 + 120 = 660 total hours.

networking solutions separating IT and OT will also fall by half to 120 hours per entity per year, for a total ongoing annual burden of 660 hours. TSA assumes the equivalent of a COM will perform the design component tasks, and a network/systems administrator and cybersecurity analyst will perform the application component of the requirements.

TSA calculates a weighted average compensation rate of $87.09 in Year 1 using a fully-loaded wage rate for a cybersecurity analyst of $71.00, for a network/system administrator of $61.21, and for a COM of $118.09 per hour.[325] In Years 2-10, TSA calculates a weighted average compensation rate of $79.67 due to the lower proportion of the time burden taken up by the COM.[326]

TSA multiplies the wage rate calculated for Year 1 by the new entity network segmentation hour burden (820 hours) and adds to it the product of the Year 2 wage rate and the existing entity network segmentation hour burden (660 hours) to calculate a network segmentation cost displayed in Table 3-63 below.

[325] TSA calculates the weighted compensation rate as ($118.09 × 320 hours) + ($71.00 × 192 hours) + ($61.21 × 288 hours) ÷ 820 hours. Value used in analysis is rounded to two decimal places.
[326] TSA calculates the weighted compensation rate as ($118.09 × 180 hours) + ($71.00 × 192 hours) + ($61.21 × 288 hours) ÷ 660 hours. Value used in analysis is rounded to two decimal places.

Table 3-63: Network Segmentation Cost for Pipelines ($ Thousands)

Year	Pipeline Population	Total Pipeline Network Segmentation Cost
	a = Column j, Table 2-1	b = {a_{Y1} × 820 hours × $87.09, a_{Yn} × 660 hours × $79.57}
1	115.00	$8,212.6
2	115.00	$6,039.4
3	115.00	$6,039.4
4	115.00	$6,039.4
5	115.00	$6,039.4
6	115.00	$6,039.4
7	115.00	$6,039.4
8	115.00	$6,039.4
9	115.00	$6,039.4
10	115.00	$6,039.4
Total		**$62,566.9**

Notes: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

The costs related to access control involve designing and reviewing necessary criteria and solutions. TSA SMEs with cybersecurity expertise estimate pipeline owner/operators would spend 100 hours in Year 1 and 58.34 hours in subsequent years (Years 2 through 10) performing this task, as discussed in Section 2.4.4.5. The time burdens include time to design the criteria, conduct an access review, and design network solutions. These tasks would be performed by a network/systems administrator, cybersecurity analyst, and the COM.

TSA calculates a weighted average compensation rate of $100.61 in Year 1 using a fully-loaded wage rate for a cybersecurity analyst of $71.00, for a network/systems administrator of $61.21, and for a COM of $118.09 per hour.[327] In Years 2 through 10, TSA calculates a weighted average compensation rate of $87.96 per hour.[328]

TSA multiplies the wage rate calculated for Year 1 by the new entity access control hour burden (100 hours) and adds to it the product of the Year 2 wage rate and the existing entity access

[327] TSA calculates the weighted compensation rate as ($118.09 × 67 hours) + ($71.00 × 13.2 hours) + ($61.21 × 19.8 hours) ÷ 100 hours. Value used in analysis is rounded to two decimal places.

[328] TSA calculates the weighted compensation rate as ($118.09 × 25 hours) + ($71.00 × 13.2 hours) + ($61.21 × 19.8 hours) ÷ 58 hours. Value used in analysis is rounded to two decimal places.

control hour burden (58.34 hours) to calculate an access control cost displayed in Table 3-64.

Table 3-64: Compliance with Access Control Cost for Pipelines ($ Thousands)

Year	Pipeline Population	Total Pipeline Access Control Cost
	a = Column j, Table 2-1	b = {a_{Y1} × 100 hours × $100.61, a_{Yn} × 58.34 hours × $87.96}
1	115.00	$1,157.0
2	115.00	$590.1
3	115.00	$590.1
4	115.00	$590.1
5	115.00	$590.1
6	115.00	$590.1
7	115.00	$590.1
8	115.00	$590.1
9	115.00	$590.1
10	115.00	$590.1
Total		**$6,468.2**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

As part of their plan to control access to Critical Cyber Systems and prevent unauthorized access, TSA estimates owner/operators would procure multi-factor authentication (MFA) software at a cost of $72 per employee as discussed in Section 2.4.7. TSA estimates owner/operators would have to acquire access control equipment and apply it to the user accounts of all their employees. TSA multiplies the cost of MFA acquisition by the employee population for pipelines identified in Section 2.1.4 to obtain an MFA equipment acquisition cost.

TSA also estimates each employee would incur a time burden each time the employee uses MFA and may incur additional time burdens to manage any lockouts or password resets needed. TSA estimates each employee a one minute per day time burden to use MFA, for a total of 4.17 hours per year, per employee.[329] TSA assumes employees would use MFA daily to log into IT network systems such as email, chat communications, file share servers, or HR systems. Since these are systems employees engage with regularly, TSA estimates that account lockouts would be rare.

[329] TSA estimates 1 min per day per employee to access MFA for a total hour burden of 4.17 hours per year, per employee. (1 ÷ 60) × 250 working days per year = 4.17 hours.

TSA estimates each employee incurs a 15-minute time burden to resolve lockouts for each occurrence and estimates each employee may experience a lockout twice every two months, for a total of 3 hours per year, per employee as discussed in Section 2.4.4.5. Together, TSA calculates each employee incurs a time burden of 7.17 hours per year due to MFA requirements. TSA estimates the cost of MFA to entities using a fully-loaded mean wage rate of $69.32 for the pipeline employee population.[330] TSA multiplies the same wage rate by the employee MFA time burden (7.17 hours) to calculate an employee MFA engagement cost as shown in Table 3-65 below.

Table 3-65: Access Control Implementation Cost for Pipelines ($ Thousands)

Year	Employee Population Plus Growth	MFA Equipment Cost	MFA Implementation Cost	Total Cost
	a = Column g, Table 2-2	b = a × $72	c = a × 7.17 hours × $69.32	d = b + c
1	39,920.00	$2,874.2	$19,841.2	$22,715.5
2	40,167.50	$2,892.1	$19,964.2	$22,856.3
3	40,416.54	$2,910.0	$20,088.0	$22,998.0
4	40,667.13	$2,928.0	$20,212.6	$23,140.6
5	40,919.26	$2,946.2	$20,337.9	$23,284.1
6	41,172.96	$2,964.5	$20,464.0	$23,428.4
7	41,428.23	$2,982.8	$20,590.8	$23,573.7
8	41,685.09	$3,001.3	$20,718.5	$23,719.8
9	41,943.54	$3,019.9	$20,847.0	$23,866.9
10	42,203.59	$3,038.7	$20,976.2	$24,014.9
Total		**$29,557.7**	**$204,040.4**	**$233,598.1**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

As part of their COIP, each owner/operator must develop a patch management strategy that ensures all critical security patches and updates for operating systems, applications, drivers and firmware are current.

TSA estimates affected entities would spend 82 hours in Year 1 and 80 hours in Years 2 through 10 performing this task as discussed in Section 2.4.4.5. TSA estimates the time burden is

[330] See Section 2.3.4.

comprised of four hours in Year 1 and two hours in subsequent years to create and maintain a patch strategy and 78 hours per entity per year to manage new patches.[331] A TSA SME with cybersecurity expertise estimates this task would be performed by the equivalent of a system/network administrator and a COM. TSA calculates a weighted average compensation rate of $63.98 per hour using a fully-loaded wage rate for a network/systems administrator of $61.21 and for a COM of $118.07 per hour as discussed in Section 2.3.4.[332] In Years 2 through 10 TSA calculates a weighted average compensation rate of $62.63 per hour due to the lower proportion of the time burden taken up by the COM.[333]

TSA uses the same wage rate from Year 1 and multiplies by the new entity patch implementation hour burden (82 hours) to yield a patch implementation cost and adds to it the product of the wage rate for existing entities in Years 2 – 10 and the existing entity patch implementation hour burden (80 hours) to yield total patch implementation cost shown in Table 3-66 below.

TSA also estimates additional owner/operator time burden due to responding to new patches. TSA estimates that each entity will need to apply patches in at least one cycle per quarter and that each entity will incur a time burden of 375 hours to complete each cycle as discussed in Section 2.4.4.5. TSA estimates this task would be performed by a system/network administrator using a fully-loaded wage rate of $61.21 per hour. Table 3-66 presents the total pipeline patching cost over 10 years. It includes new entity patching, existing entity patching, and cost to respond to new patches.

---

[331] TSA SMEs with cybersecurity expertise estimate each owner/operator would spend approximately 1.5 hours per week checking CISA's list of known vulnerabilities.

[332] TSA calculates the weighted compensation rate as ($118.09 × 4 hours) + ($61.21 × 78 hours) ÷ 82 hours. Value used in analysis is rounded to two decimal places.

[333] TSA calculates the weighted compensation rate as ($118.09 × 2 hours) + ($61.21 × 78 hours) ÷ 80 hours. Value used in analysis is rounded to two decimal places.

Table 3-66: Patching Implementation Cost for Pipelines ($ Thousands)

Year	Pipeline Population	Patching Costs	Cost to Respond to New Patches	Total Pipeline Patching Cost
	a = Column j, Table 2-1	b = {a_{Y1} × 82 hours × $63.98, a_{Yn} × 80 hours × $62.63}	c = a × 4 patching cycles per year × 375 hours per cycle × $61.21	d = b + c
1	115.00	$603.3	$10,558.7	$11,162.1
2	115.00	$576.2	$10,558.7	$11,134.9
3	115.00	$576.2	$10,558.7	$11,134.9
4	115.00	$576.2	$10,558.7	$11,134.9
5	115.00	$576.2	$10,558.7	$11,134.9
6	115.00	$576.2	$10,558.7	$11,134.9
7	115.00	$576.2	$10,558.7	$11,134.9
8	115.00	$576.2	$10,558.7	$11,134.9
9	115.00	$576.2	$10,558.7	$11,134.9
10	115.00	$576.2	$10,558.7	$11,134.9
Total		**$5,789.1**	**$105,587.3**	**$111,376.3**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

Finally, TSA estimates the cost of data backups for Critical Cyber Systems includes the cost to acquire the necessary storage space for all Critical Cyber System data backed up and the time burden to supervise the backup process. A TSA SME with cybersecurity expertise estimates an average Critical Cyber System data volume per entity in Year 1 of 500 terabytes (TB) of data.[334] TSA estimates the storage cost per TB of data backed up as $329.16 per TB per year.[335] TSA assumes entities will use a cloud-based provider to store Critical Cyber System backup data. TSA is aware that alternatives exist for affected entities and that owner/operators may not choose to store their Critical Cyber System backup data in a cloud environment. TSA invites public comment on these cost assumptions. TSA further estimates that the volume of Critical Cyber System data held by pipeline entities would grow in Years 2 through 10. TSA calculates a

[334] TSA assumes affected entities will purchase cloud-based storage sufficient to meet their Critical Cyber System data backup needs in advance at the beginning of each year. TSA request comment on the amount of storage space owner-operators will need.

[335] "Cloud Storage Pricing in 2023: Everything You Need to Know." Anina Ot. Accessed September 26, 2023. https://www.enterprisestorageforum.com/cloud/cloud-storage-pricing/. TSA uses the above article's "Cloud Storage Pricing Chart" to compare five of the six (U.S.-based) cloud storage providers. The table's final row provides a per month per TB cost estimator. The article's five point estimates average to $27.43 per TB per month (($34.67 + $24.90 + $24.08 + $26.40 + $27.00) ÷ 5). TSA multiplies the per month amount by 12 months to yield an annual cost of $329.16 per TB per year.

compound annual growth rate of Critical Cyber System data volume of 2.3 percent per year between Years 2 through 10.[336]

Once the backup is complete, the data will need to be safely stored. TSA cybersecurity SMEs estimate that each backup would need to be stored for a period of one year. TSA scales the per TB per month cost above appropriately.[337] TSA also estimates the cost associated with the time burden on pipeline entities to supervise the backup of their data. A TSA SME with cybersecurity expertise estimates that each entity would require 12 hours per year (1 hour per month) to supervise the backup of their Critical Cyber System data. TSA calculates a fully loaded wage for a network/systems administrator of $61.21 per hour to supervise the backup of Critical Cyber System data.

TSA multiplies the network/systems administrator wage rate by the backup supervision hour burden (12 hours) to yield a data backup supervision cost. Table 3-67 presents pipeline critical system backup costs over time. It includes cost of data storage and time for backup supervision.

---

[336] Alex Woodie. "Big Growth Forecasted for Big Data." https://www.datanami.com/2022/01/11/big-growth-forecasted-for-big-data/#:~:text=From%202020%20to%202025%2C%20IDC,of%20data%20creation%20by%202025. Accessed July 3, 2023. TSA extracted a forecast that raw data creation is expected to grow at a compound annual rate of 23% per year per entity between 2020 and 2025. However, the author also notes that organizations only save into long-term storage roughly 10% of the data which they create each year. Therefore, the net compound annual growth rate applicable to data storage needs is 23% × 10% = 2.3% per year. TSA understands this average may not capture the exact circumstances for all industries. TSA invites public comment on this input.

[337] "Cloud Storage Pricing in 2023: Everything You Need to Know." Anina Ot. Accessed September 26, 2023. https://www.enterprisestorageforum.com/cloud/cloud-storage-pricing/.

Table 3-67: Critical System Data Backup Costs for Pipelines ($ Thousands)

Year	Pipeline Population	Critical System Data Size Per Entity (Terabytes)	Cost of Data Backups	Cost of Data Backup Supervision	Total Cost of Pipeline Critical System Data Backups
	a = Column j, Table 2-1	b = 500 × (1+ 2.30%)^Y_{n-1}	c = a × b × $329.16	d = a × 12 hours × $61.21	e = c + d
1	115.00	500.00	$18,926.7	$84.5	$19,011.2
2	115.00	511.50	$19,362.0	$84.5	$19,446.5
3	115.00	523.26	$19,807.2	$84.5	$19,891.6
4	115.00	535.29	$20,262.5	$84.5	$20,347.0
5	115.00	547.60	$20,728.5	$84.5	$20,813.0
6	115.00	560.19	$21,205.1	$84.5	$21,289.6
7	115.00	573.07	$21,692.6	$84.5	$21,777.1
8	115.00	586.25	$22,191.6	$84.5	$22,276.0
9	115.00	599.73	$22,701.8	$84.5	$22,786.3
10	115.00	613.52	$23,223.8	$84.5	$23,308.3
Total			**$210,101.9**	**$844.7**	**$210,946.6**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed. Formulas with X_{yn-1} in year one are equal to the initial value of X_{y1}.

3.4.5.6 Training Cost

This provision requires owner/operators to provide all employees and contractors with access to the owner/operator's IT or OT systems basic cybersecurity training that includes cybersecurity awareness to address cyber-hygiene best practices, acceptable use, risks associated with their level of privileged access, and awareness of security risks associated with their actions. The owner/operator must also provide additional role-based training to cybersecurity-sensitive employees. The cost of this provision relates to four areas, including each entity's time burden to develop and implement its cybersecurity training plans, time burdens to all employees to take basic user training, time burdens to privileged users to take role-based training, and recordkeeping.

Each owner/operator must develop, submit, and implement their cybersecurity training plans. TSA estimates all covered pipeline entities would spend 80 hours to develop and implement their

cybersecurity training plans.[338] TSA estimates that this task would be performed by a pipeline COM using a fully-loaded wage rate of $118.09 per hour.

TSA multiplies the same wage rate by the submission hour burden (80 hours) and the entity population to generate a cybersecurity training plan development cost as shown in Table 3-68 below.

Table 3-68: Cybersecurity Training Plan Costs - Pipelines ($ Thousands)

Year	Pipeline Initial Submissions	Pipeline Total Training Plan Cost
	a_{Y1} = 115.00 a_{yn} = 0	b = a × 80 hours × $118.09
1	115.00	$1,086.43
2	-	$0.00
3	-	$0.00
4	-	$0.00
5	-	$0.00
6	-	$0.00
7	-	$0.00
8	-	$0.00
9	-	$0.00
10	-	$0.00
Total		**$1,086.4**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

Basic User Awareness Training is intended to provide effective cybersecurity awareness training that helps employees understand proper cyber-hygiene and the security risks associated with their actions. TSA estimates each employee would spend one hour per year completing this training.[339] TSA estimates that 100 percent of the affected pipeline employee population will require basic user training, while 15 percent will require role-based training. TSA calculates basic user awareness training by multiplying the pipeline employee population by the one hour training burden, and the fully-loaded general pipeline wage rate of $69.32 per hour as described

[338] See "Security Training Programs for Surface Transportation Employees – Final Rulemaking." RIN: 1652-AA55. Regulatory Impact Analysis. Page 57. TSA expects the burden hours for the initial submission of the Cybersecurity training plan to be comparable to the burden hours from the Physical Security rulemaking due to the similar length and breadth of requirements, as well as that entities may not yet have experience producing such plans.

[339] TSA SMEs with cybersecurity expertise estimate one (1) hour for employee training as a baseline.

in Section 2.3.4.

Role-based training would consider the role of the privileged user in a cyber-incident~~,~~ as such users bring a unique level of risk to an organization. A privileged user is one that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform. TSA SMEs with cybersecurity expertise estimate the privileged user population as 15 percent of the general user population. TSA SMEs with cybersecurity expertise estimate privileged users would spend two hours per year completing this training. TSA calculates role-based training costs by multiplying the pipeline privileged user population, by the two hour training burden and the fully-loaded pipeline privileged user wage rate of $67.44 per hour described in Section 2.3.4 for the pipeline privileged user population.

Finally, each owner/operator would be required to retain records of initial and recurrent cybersecurity training for everyone required to receive such training. TSA estimates owner/operators would spend 0.02 hours per record handling records, for both basic user awareness training records and role-based training records.[340] TSA calculates training recordkeeping costs by multiplying the number of trainings per year by the 0.02 hour training recordkeeping burden, and the fully loaded administrative assistant's wage rate of $40.63 per hour described in Section 2.3.4.

Table 3-69 presents cybersecurity training costs for pipeline over 10 years. It includes general training, role-based training, and recordkeeping costs.

[340] TSA assumes an administrative assistant for each owner/operator would file a record of each employee's training session. TSA estimates a duration of one-minute (~0.02 hours) for an administrative staff person to file a training record.

Table 3-69: Cybersecurity Training Costs for Pipelines ($ Thousands)

Year	Pipeline Training Population	General Training Cost	Role-Based Training Cost	Training Recordkeeping Cost	Total Cybersecurity Training Cost
	a = Column g, Table 2-2	b = a × 1 hour × $69.32	c = a x 15% × 2 hours × $67.44	d = (a + (a × 15%)) × 0.02 hours × $40.63	e = b + c + d
1	39,920.00	$2,767.3	$807.7	$37.3	$3,612.2
2	40,167.50	$2,784.4	$812.7	$37.5	$3,634.6
3	40,416.54	$2,801.7	$817.7	$37.8	$3,657.2
4	40,667.13	$2,819.0	$822.8	$38.0	$3,679.8
5	40,919.26	$2,836.5	$827.9	$38.2	$3,702.6
6	41,172.96	$2,854.1	$833.0	$38.5	$3,725.6
7	41,428.23	$2,871.8	$838.2	$38.7	$3,748.7
8	41,685.09	$2,889.6	$843.4	$39.0	$3,771.9
9	41,943.54	$2,907.5	$848.6	$39.2	$3,795.3
10	42,203.59	$2,925.6	$853.9	$39.4	$3,818.9
Total		**$28,457.5**	**$8,305.7**	**$383.6**	**$37,146.9**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

3.4.5.7 Detection of Cybersecurity Incidents Cost

Under the proposed rule, owner/operators must incorporate into their COIP policies, procedures, and capabilities sufficient to detect and respond to cybersecurity threats and anomalies on Critical Cyber Systems. These policies, procedures, and capabilities must defend against malicious email, block ingress and egress communications, control the impact of known or suspected malicious web domains or applications, block and defend against unauthorized code or malicious command and control servers, and ensure continuous collection and analysis of data for potential intrusions and anomalous behavior. TSA estimates each affected entity would spend 106.5 hours in Year 1 and 100.5 hours in Years 2 through 10 performing these tasks.[341] In Year 1, this includes four hours to design continuous monitoring criteria, eight hours to develop solutions for IT, two hours per quarter for four network/systems administrators to meet to review

[341] TSA consulted SMEs with cybersecurity expertise and determined that an hour burden range of 106.5 – 211 hours for Year 1 and a range of 100.5 – 197 hours for Years 2-10. TSA uses the lower range estimates as it believes average costs would be closer to the lower values.

security threats (a total of 32 hours per year), and 15 minutes per work day for updates to the list of blocked websites (a total of 62.5 hours per year).[342] For Years 2 through 10, TSA estimates there would be efficiency gains from experience implementing these process. In Years 2 through 10 TSA estimates each affected entity will spend two hours to design the criteria, four hours to develop solutions for IT, and the continuation of the quarterly meetings and daily updates for an annual burden of 100.50 hours. TSA assumes these tasks would be performed by the COM and network/systems administrator.

TSA calculates a weighted average compensation rate of $67.62 per hour in Year 1 using the fully-loaded wage rate for a COM of $118.09 and for a network/systems administrator of $61.21 per hour.[343] TSA calculates a weighted average compensation rate of $64.61 in Years 2 through 10 due to lower participation of the cybersecurity coordinator in the time burden.[344]

TSA also estimates an annual cost of $2,995 per owner/operator for the software necessary for continuous monitoring as discussed in Section 2.4.4.8. Table 3-70 presents continuous monitoring pipeline costs over 10 years. It includes new entity monitoring costs, existing entity monitoring costs, and software costs.

---

[342] TSA calculates the estimated time burden as 4 hours + 8 hours + (2 hours × 4 quarters × 4 network/systems administrators = 32 hours) + (15 minutes per day × 250 working days per year) ÷ 60 minutes = 62.5 hours) = 106.5 hours in Year 1

[343] TSA calculates the weighted compensation rate as ($118.09 × 12 hours) + ($61.21 × 94.5 hours) ÷ 106.5 hours. Value used in analysis is rounded to two decimal places.

[344] TSA calculates the weighted compensation rate as ($118.09 × 6 hours) + ($61.21 × 94.5 hours) ÷ 100.5 hours. Value used in analysis is rounded to two decimal places.

Table 3-70: Continuous Monitoring Cost for Pipelines ($ Thousands)

Year	Pipeline Population	Continuous Monitoring Cost	Software Cost	Total Pipeline Continuous Monitoring Cost
	a = Column j, Table 2-1	b = {a_{y1} × 106.5 hours × $67.62, a_{yn} × 100.5 hours × $64.61}	c = a × $2,995	d = b + c
1	115.00	$828.2	$344.43	$1,172.6
2	115.00	$746.7	$344.43	$1,091.2
3	115.00	$746.7	$344.43	$1,091.2
4	115.00	$746.7	$344.43	$1,091.2
5	115.00	$746.7	$344.43	$1,091.2
6	115.00	$746.7	$344.43	$1,091.2
7	115.00	$746.7	$344.43	$1,091.2
8	115.00	$746.7	$344.43	$1,091.2
9	115.00	$746.7	$344.43	$1,091.2
10	115.00	$746.7	$344.43	$1,091.2
Total				**$10,993.0**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

3.4.5.8 Capabilities to Respond to a Cybersecurity Incident

This provision details additional requirements that owner/operators must include in their COIP capabilities when it comes to responding to cybersecurity incidents that affect Critical Cyber Systems. These specifics are discussed in Section 2.4.4.6 and the time necessary to address these requirements is incorporated into the overall plan development estimates, which is accounted for and discussed in Section 3.4.5.

3.4.5.9 Plan of Action and Milestones (POAM) Cost

Owner/operators who are unable to meet every requirement and security outcome required by the COIP must create a POAM that includes policies, procedures, measures, or capabilities that the owner/operator will develop to ensure all requirements are met. Due to the constantly changing cybersecurity environment, TSA expects a portion of owner/operators would be unable to meet every requirement and security outcome each year and would be required to complete a POAM. As a result of existing voluntary frameworks and compliance with the SDs, TSA estimates 20 percent of owner/operators would need to complete a POAM in the first three years of the rule and that would take 80 hours to complete (see Section 2.4.4.10). TSA invites comment on the

proportion of owner/operators who would need to complete a POAM. TSA SMEs with cybersecurity expertise estimate a network/systems administrator would spend 48 hours on this task while a cybersecurity analyst will spend 32 hours.

TSA calculates a weighted average compensation rate of $65.13 per hour using the fully-loaded wage rate for a network/systems administrator of $61.21 and of $71.00 per hour for the cybersecurity analyst.[345] TSA multiplies average compensation rate by the POAM hour burden (80 hours) and the affected pipeline entity population to yield the 10-year POAM cost, as shown in Table 3-71 below.

Table 3-71: Plan of Action and Milestones (POAM) Cost for Pipelines ($ Thousands)

Year	Pipeline Population	Pipeline Population	Total POAM Cost for Pipeline
	a = Column j, Table 2-1	b = {a × 20%, 0}	c = b × 80 hours × $65.13
1	115.00	23.00	$119.8
2	115.00	23.00	$119.8
3	115.00	23.00	$119.8
4	115.00	0	$0.0
5	115.00	0	$0.0
6	115.00	0	$0.0
7	115.00	0	$0.0
8	115.00	0	$0.0
9	115.00	0	$0.0
10	115.00	0	$0.0
Total			**$359.5**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

3.4.5.10 Total Cost of the COIP

TSA estimates the total cost impact of all COIP components for Pipeline entities as $722 million undiscounted over 10 years as presented in Table 3-72 below. The table also presents the total cost of each provision as a percent of total COIP costs. The cost of Critical System Data Backups and MFA Use represents the largest share of COIP costs at 29.2 percent and 28.3 percent.

[345] TSA calculates the weighted compensation rate as ($61.21 × 48 hours) + ($71.00 × 32 hours) ÷ 80 hours. Value used in analysis is rounded to two decimal places.

Table 3-72: Total COIP Cost for Pipelines ($ Thousands)

Year	COIP Development and Accountable Executive Designation	Cybersecurity Coordinator Designation	Identification of Critical Cyber Systems	Supply Chain Risk Management	Network Segmentation	Access Control			Patching	Critical System Data Backups	Cybersecurity Training	Detection of Cybersecurity Incidents	POAM	Total Cost of the COIP for Pipeline
						Compliance	MFA Equipment	MFA Implementation						
	Table 3-59	Table 3-60	Table 3-61	Table 3-62	Table 3-63	Table 3-64	Column b, Table 3-65	Column c, Table 3-65	Table 3-66	Table 3-67	Table 3-68 + Table 3-69	Table 3-70	Table 3-71	
1	$994.1	$91.6	$1,703.7	$3,747.6	$8,212.6	$1,157.0	$2,874.2	$19,841.2	$11,162.1	$19,011.2	$4,698.6	$1,172.6	$119.8	$74,786.3
2	$316.0	$12.5	$425.9	$3,747.6	$6,039.4	$590.1	$2,892.1	$19,964.2	$11,134.9	$19,446.5	$3,634.6	$1,091.2	$119.8	$69,414.8
3	$316.0	$12.5	$425.9	$3,747.6	$6,039.4	$590.1	$2,910.0	$20,088.0	$11,134.9	$19,891.6	$3,657.2	$1,091.2	$119.8	$70,024.2
4	$316.0	$12.5	$425.9	$3,747.6	$6,039.4	$590.1	$2,928.0	$20,212.6	$11,134.9	$20,347.0	$3,679.8	$1,091.2	$0.0	$70,525.0
5	$316.0	$12.5	$425.9	$3,747.6	$6,039.4	$590.1	$2,946.2	$20,337.9	$11,134.9	$20,813.0	$3,702.6	$1,091.2	$0.0	$71,157.2
6	$316.0	$12.5	$425.9	$3,747.6	$6,039.4	$590.1	$2,964.5	$20,464.0	$11,134.9	$21,289.6	$3,725.6	$1,091.2	$0.0	$71,801.1
7	$316.0	$12.5	$425.9	$3,747.6	$6,039.4	$590.1	$2,982.8	$20,590.8	$11,134.9	$21,777.1	$3,748.7	$1,091.2	$0.0	$72,457.0
8	$316.0	$12.5	$425.9	$3,747.6	$6,039.4	$590.1	$3,001.3	$20,718.5	$11,134.9	$22,276.0	$3,771.9	$1,091.2	$0.0	$73,125.3
9	$316.0	$12.5	$425.9	$3,747.6	$6,039.4	$590.1	$3,019.9	$20,847.0	$11,134.9	$22,786.3	$3,795.3	$1,091.2	$0.0	$73,806.0
10	$316.0	$12.5	$425.9	$3,747.6	$6,039.4	$590.1	$3,038.7	$20,976.2	$11,134.9	$23,308.3	$3,818.9	$1,091.2	$0.0	$74,499.5
Total	**$3,837.7**	**$204.3**	**$5,536.9**	**$37,475.6**	**$62,566.9**	**$6,468.2**	**$29,557.7**	**$204,040.4**	**$111,376.3**	**$210,946.6**	**$38,233.3**	**$10,993.0**	**$359.5**	**$721,596.4**
% of Total	0.5%	0.0%	0.8%	5.2%	8.7%	0.9%	4.1%	28.3%	15.4%	29.2%	5.3%	1.5%	0.0%	100.0%

Note: Totals may not add due to rounding.

3.4.6 Reporting Cybersecurity Incidents Cost

Under the proposed rule, owner/operators would be required to report any cybersecurity incident, as defined in the TSA Cybersecurity Lexicon, to CISA as soon as practicable, but no later than 24 hours after a cybersecurity incident is identified. The reporting entity must include the contact information of the reporting individual, the affected systems, a description of the incident and threat, earliest known date of compromise, date of detection and other relevant information. TSA SMEs with cybersecurity expertise utilize internal data relating to reportable incidents to estimate 3.48 reportable cybersecurity incidents per year per owner/operator as discussed in Section 2.4.10. TSA estimates that each affected entity would incur a one hour time burden to report each incident.[346] TSA SMEs with cybersecurity experience expect the one hour time burden would be split equally between a cybersecurity analyst and a COM.

TSA calculates a weighted average compensation rate of $94.55 per hour using a fully-loaded wage rate for a cybersecurity analyst of $71.00 and for a COM of $118.09 per hour as discussed in Section 2.3.4.[347]

TSA then multiplies the weighted average compensation rate ($94.55) by the incident reporting hour burden (1 hour) number of pipelines per year, and expected incident reporting volume to calculate a pipeline cybersecurity incident reporting costs.

Table 3-73 presents the total pipeline cybersecurity incident reporting cost over 10 years.

[346] This is consistent with the value in ICR 1652-0051 (Rail Security), which estimated 1 hour to report "significant security concerns."

[347] TSA calculates the weighted compensation rate as ($118.09 × 0.5 hours) + ($71.00 × 0.5 hours). Value used in analysis is rounded to two decimal places.

Table 3-73: Cybersecurity Incident Reporting Cost for Pipelines ($ Thousands)

Year	Pipeline Affected Population	Number of Reported Cybersecurity Incidents	Cost to Report Incidents
	a = Column j, Table 2-1	b = a × 3.48	c = b × 1 hour × $94.55
1	115.00	400.20	$37.8
2	115.00	400.20	$37.8
3	115.00	400.20	$37.8
4	115.00	400.20	$37.8
5	115.00	400.20	$37.8
6	115.00	400.20	$37.8
7	115.00	400.20	$37.8
8	115.00	400.20	$37.8
9	115.00	400.20	$37.8
10	115.00	400.20	$37.8
Total			$378.4

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

3.4.7 Cybersecurity Incident Response Plan (CIRP) Cost

Under the proposed rule, each affected owner/operator must develop and maintain a CIRP to be filed with TSA. The CIRP must provide specific measures to ensure prompt isolation and segregation of the infected system from the uninfected systems, address the security and integrity of backed-up data, establish capability and governance for implementing mitigation measures, identify which individual is responsible for implementing the CIRP, and conduct exercises to test the plan's effectiveness. TSA estimates that the COM of each affected owner/operator would spend 80 hours in Year 1 to develop the plan and 20 hours in each subsequent year to maintain the plan.

TSA multiplies the COM fully-loaded wage rate of $118.09 per hour discussed in Section 2.3.4 by CIRP development time burden (80 hours) and the number of new pipeline entities to estimate CIRP development costs. TSA multiplies the same wage rate by the CIRP maintenance hour burden (20 hours) and number of existing pipelines to calculate CIRP maintenance costs. Table 3-74 presents pipeline CIRP costs over ten years. It includes initial CIRP development costs and CIRP annual maintenance costs.

In addition, TSA estimates owner/operators would spend an average of 120 hours to test the effectiveness of their CIRP. TSA assumes this testing would be completed by the equivalent of a COM. TSA multiples the fully loaded COM wage rate of $118.09 per hour from Section 2.3.4, CIRP effectiveness testing hour burden (120 hours), and number of pipeline owner/operators to calculate CIRP effectiveness testing costs per year.

Table 3-74: Cybersecurity Incident Response Plan (CIRP) Costs for Pipeline ($ Thousands)

Year	Pipeline Population	CIRP Cost	CIRP Effectiveness Testing Cost	Total Cost
	a = Column j, Table 2-1	b = {a_{Y1} x 80 hours x $118.09, a_{Yn} × 20 hours × $118.09}	c = a × 120 hours × $118.09	d = b + c
1	115.00	$1,086.4	$1,629.6	$2,716.1
2	115.00	$271.6	$1,629.6	$1,901.2
3	115.00	$271.6	$1,629.6	$1,901.2
4	115.00	$271.6	$1,629.6	$1,901.2
5	115.00	$271.6	$1,629.6	$1,901.2
6	115.00	$271.6	$1,629.6	$1,901.2
7	115.00	$271.6	$1,629.6	$1,901.2
8	115.00	$271.6	$1,629.6	$1,901.2
9	115.00	$271.6	$1,629.6	$1,901.2
10	115.00	$271.6	$1,629.6	$1,901.2
Total		**$3,530.9**	**$16,296.4**	**$19,827.3**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

In addition, each entity would implement its CIRP following a cyber incident. TSA estimates each entity would spend 160 hours per incident to implement its CIRP as discussed in Section 2.4.6. TSA estimates 60 percent of the hour burden would be performed by a network/systems administrator and 40 percent of the hour burden would be performed by a cybersecurity analyst.[348] TSA calculates a weighted average compensation rate of $65.13 per hour using a fully-loaded wage for a cybersecurity analyst of $71.00 per hour and for a network/systems administrator of $61.21 per hour as discussed in Section 2.3.4.[349] TSA multiplies the weighted

[348] TSA calculates the estimated time burdens as (160 hours × 0.60 = 96 hours) and (160 hours × 0.40 = 64 hours).
[349] TSA calculates the weighted compensation rate as ($71.00 × 64 hours) + ($61.21 × 96 hours) ÷ 160 hours. Value used in analysis is rounded to two decimal places.

average compensation rate ($65.13) by the CIRP implementation hour burden (160 hours) and the number of freight railroads cybersecurity incidents per year to calculate freight rail CIRP costs as shown in Table 3-75 below.

Table 3-75: Cybersecurity Incident Response Plan (CIRP) Cost for Pipelines ($ Thousands)

Year	Pipeline Affected Population	Number of Cybersecurity Incidents	Cost to Respond to Incidents
	a = Column j, Table 2-1	b = a x 3.48	c = b x 160 hours x $65.13
1	115.00	400.20	$4,170.4
2	115.00	400.20	$4,170.4
3	115.00	400.20	$4,170.4
4	115.00	400.20	$4,170.4
5	115.00	400.20	$4,170.4
6	115.00	400.20	$4,170.4
7	115.00	400.20	$4,170.4
8	115.00	400.20	$4,170.4
9	115.00	400.20	$4,170.4
10	115.00	400.20	$4,170.4
Total			**$41,704.0**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

3.4.8 Cybersecurity Assessment Plan (CAP) Cost

Under the proposed rule, each owner/operator must develop and maintain a Cybersecurity Assessment Plan (CAP) to be filed with an approved by TSA. The CAP must proactively assess the effectiveness of the COIP, and identify and resolve vulnerabilities associated with identified Critical Cyber Systems, including device, network, or other identified vulnerabilities. TSA estimates that the equivalent of a cybersecurity analyst would spend 40 hours to develop the CAP and a COM and network/systems administrator will each spend two hours reviewing the CAP.[350]

TSA calculates a weighted average compensation rate of $72.70 per hour using the fully-loaded wage rate for a COM of $118.09, a cybersecurity analyst of $71.00, and a network/systems

[350] TSA calculates the estimated time burden as 40 hours for the cybersecurity analyst + (2 hours × 2 cybersecurity coordinators) = 44 total hours

administrator of $61.21 per hour as discussed in Section 2.3.4.[351] TSA multiplies the average compensation rate by the CAP creation hour burden (44 hours) and the pipeline entity population as shown in Table 3-76 below.

In addition, each entity would implement its CAP by conducting architectural design review (ADR) and penetration testing every two years, beginning in Year 2. While penetration testing is not a stated rule requirement, TSA is including representative costs to reflect actions that may be taken by companies as a part of their processes to be in full compliance with the provisions of the proposed rule in pursuit of a strong CRM program. TSA estimates each entity will conduct penetration testing upon its second full year in the population. TSA estimates each entity would spend 40 hours to conduct the ADR and implement the CAP, with 24 hours attributed to the network/systems administrator and 16 hours attributed to the cybersecurity analyst as discussed in Section 2.4.7. TSA estimates that in addition to the ADR time burden, each entity would incur a flat cost of $20,000 every two years to conduct penetration testing (see Section 2.4.7). [352] TSA estimates each entity would only conduct ADR and penetration testing every 2 years. TSA assumes existing entities would conduct such activities in the 2nd full year after the implementation of the rule. In years between these periods, no existing entities would conduct activities.

TSA calculates a weighted average compensation rate of $65.13 per hour using the fully-loaded wage rate for a cybersecurity analyst of $71.00 and for a network/systems administrator of

[351] TSA calculates the weighted compensation rate as ($71.00 × 10 hours) + ($118.09 × 2 hours) + ($61.21 × 2 hours) ÷ 14 hours. Value used in analysis is rounded to two decimal places.
[352] RSI Security. What Is The Average Cost Of Penetration Testing?. May 5, 2023, available at https://blog.rsisecurity.com/what-is-the-average-cost-of-penetration-testing/. Accessed September 25, 2023.

$61.21 per hour as discussed in Section 2.3.4.[353]

TSA calculates the cost of ADR using the previously described compensation rate multiplied by the ADR hour burden (20 hours) and ADR two-year cycle. TSA similarly estimates penetration testing by multiplying the two-year cycle by the cost of penetration testing ($20,000). Table 3-76 below presents pipeline CAP costs over 10 years.

Table 3-76: Cybersecurity Assessment Plan (CAP) Cost for Pipelines ($ Thousands)

Year	Pipeline Population	Population for Penetration Testing	Cost to Develop CAP	Cost of Penetration Testing	Total Cost
	a = Column j, Table 2-1	b = {0, a_{y1}}	c = a x 44 hours x $72.70	d = (b x 40 hours x $65.13) + (b x $20,000)	e = c + d
1	115.00	0	$367.9	$0.0	$367.9
2	115.00	115	$367.9	$2,599.6	$2,967.5
3	115.00	0	$367.9	$0.0	$367.9
4	115.00	115	$367.9	$2,599.6	$2,967.5
5	115.00	0	$367.9	$0.0	$367.9
6	115.00	115	$367.9	$2,599.6	$2,967.5
7	115.00	0	$367.9	$0.0	$367.9
8	115.00	115	$367.9	$2,599.6	$2,967.5
9	115.00	0	$367.9	$0.0	$367.9
10	115.00	115	$367.9	$2,599.6	$2,967.5
Total			**$3,678.6**	**$12,998.0**	**$16,676.6**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

The CAP must also include a schedule to ensure completion of planned assessments. The schedule must ensure at least 30 percent of the policies, procedures, measures, and capabilities in the COIP are assessed each year and 100 percent are assessed every three years. TSA SMEs with cybersecurity expertise estimate that each owner/operator would incur a time burden of 30 hours annually, or 90 hours over three years, to test the COIP. TSA also estimates a network/systems administrator would incur 18 hours of this time, while a cybersecurity analyst would incur the

[353] TSA calculates the weighted compensation rate as ($71.00 × 8 hours) + ($61.21 × 12 hours) ÷ 20 hours. Value used in analysis is rounded to two decimal places.

remaining 12 hours. In addition to this time burden, TSA estimates that each entity will incur a flat cost of $6,667 annually, or $20,000 over three years, to test the COIP as discussed in Section 2.4.7.

TSA calculates a weighted average compensation rate of $65.13 per hour using the fully-loaded wage rate for a cybersecurity analyst of $71.00 and for a network/systems administrator of $61.21 per hour as discussed in Section 2.3.4.[354]

TSA multiplies this compensation rate by COIP testing hour burden (30 hours) and the pipeline entity population to calculate COIP administrative costs. TSA then multiplies COIP testing ($6,667) by the pipeline entity population. Table 3-77 shows the total pipeline COIP testing costs over ten years.

Table 3-77: COIP Testing Cost for Pipeline ($ Thousands)

Year	Pipeline Population	Administrative Cost	Cost of Testing	Total Cost of COIP Testing
	a = Column j, Table 2-1	b = a x 30 hour x $65.13	c = a x $6,667	d = b + c
1	115	$224.7	$766.7	$991.4
2	115	$224.7	$766.7	$991.4
3	115	$224.7	$766.7	$991.4
4	115	$224.7	$766.7	$991.4
5	115	$224.7	$766.7	$991.4
6	115	$224.7	$766.7	$991.4
7	115	$224.7	$766.7	$991.4
8	115	$224.7	$766.7	$991.4
9	115	$224.7	$766.7	$991.4
10	115	$224.7	$766.7	$991.4
Total		**$2,247.0**	**$7,666.7**	**$9,913.7**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

3.4.9 Documentation to Establish Compliance

Each owner/operator would incur various recordkeeping costs, including retaining documents

[354] TSA calculates the weighted compensation rate as ($71.00 × 2.67 hours) + ($61.21 × 4 hours) ÷ 6.67 hours. Value used in analysis is rounded to two decimal places.

that would be created as part of the CRM process as well as accessing and making these documents available to TSA, as requested. TSA estimates each affected entity would spend two hours of administrative assistant time annually to meet these obligations. TSA multiplies an administrative assistant fully-loaded wage rate of $40.63 as discussed in Section 2.3.4 by the recordkeeping hour burden (2 hours) and the pipeline entity population to calculate a recordkeeping cost, as shown in Table 3-78 below.

While some of the necessary compliance parameters would be covered under specific rule provisions as part of efforts to comply with the requirements of this proposed rule, TSA additionally estimates an audit manager would incur 40 hours of time to ensure overall compliance with the full rule each year. TSA multiplies an audit manager fully-loaded wage rate of $138.10, as discussed in Section 2.3.4, by the compliance hour burden (40 hours) and the pipeline population to calculate a compliance cost, as shown in Table 3-78, below.

Table 3-78: Recordkeeping and Compliance Costs for Pipelines ($ Thousands)

Year	Pipeline Population	CRM Recordkeeping (Administrative Assistant)	CRM Compliance (Audit Manager)	Total Pipeline Recordkeeping Cost
	a = Column j, Table 2-1	b = a × 2 hours × $40.63	c = a × 40 hours × $138.10	d = b + c
1	115.00	$9.3	$635.3	$644.6
2	115.00	$9.3	$635.3	$644.6
3	115.00	$9.3	$635.3	$644.6
4	115.00	$9.3	$635.3	$644.6
5	115.00	$9.3	$635.3	$644.6
6	115.00	$9.3	$635.3	$644.6
7	115.00	$9.3	$635.3	$644.6
8	115.00	$9.3	$635.3	$644.6
9	115.00	$9.3	$635.3	$644.6
10	115.00	$9.3	$635.3	$644.6
Total		**$93.4**	**$6,352.6**	**$6,446.0**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

3.4.10 Total Cost Impact to Pipeline Transportation

TSA estimates the total cost impact of all proposed rule requirements for pipeline entities as

$827.4 million undiscounted over ten years, $705.2 million discounted at 3 percent, and $580.2 million discounted at 7 percent. Table 3-79 shows the total cost of the CRM program, which includes costs related to the CSE, COIP, CAP, Recordkeeping, and Compliance. In Table 3-80 TSA aggregates the various proposed rule costs cost discussed above including Familiarization; Physical Security costs; the CRM Program; Incident Reporting; and the CIRP. Table 3-80 also presents the percent of total cost for pipelines of each cost category.

Table 3-79: Summary of CRM Program Costs - Pipelines ($ Thousands)

Year	CSE	COIP	CAP	Recordkeeping and Compliance	Total Cost of CRM for Pipeline
	a = Table 3-57	b = Table 3-72	c = Table 3-76 + Table 3-77	d = Table 3-78	e = ∑a,b,c,d
1	$973.1	$74,786.3	$1,359.2	$644.6	$77,763.3
2	$973.1	$69,414.8	$3,958.8	$644.6	$74,991.3
3	$973.1	$70,024.2	$1,359.2	$644.6	$73,001.1
4	$973.1	$70,525.0	$3,958.8	$644.6	$76,101.5
5	$973.1	$71,157.2	$1,359.2	$644.6	$74,134.2
6	$973.1	$71,801.1	$3,958.8	$644.6	$77,377.7
7	$973.1	$72,457.0	$1,359.2	$644.6	$75,434.0
8	$973.1	$73,125.3	$3,958.8	$644.6	$78,701.9
9	$973.1	$73,806.0	$1,359.2	$644.6	$76,783.0
10	$973.1	$74,499.5	$3,958.8	$644.6	$80,076.1
Total	**$9,731.4**	**$721,596.4**	**$26,590.3**	**$6,446.0**	**$764,364.1**

Note: Totals may not add due to rounding.

Table 3-80: Total Costs for All Requirements - Pipelines ($ Thousands)

Year	Familiarization	Physical Security Costs	CRM Program				Reporting Cybersecurity Incidents	CIRP	Total Cost		
			CSE	COIP	CAP	Recordkeeping and Compliance			i = ∑a,b,c,d,e,f,g,h		
	a	b	c	d	e	f	g	h	Undiscounted	Discounted at 3%	Discounted at 7%
1	$911.6	$37.0	$973.1	$74,786.3	$1,359.2	$644.6	$37.8	$6,886.5	$85,636.2	$83,141.9	$80,033.8
2	$0.0	$21.4	$973.1	$69,414.8	$3,958.8	$644.6	$37.8	$6,071.7	$81,122.2	$76,465.5	$70,855.3
3	$0.0	$21.4	$973.1	$70,024.2	$1,359.2	$644.6	$37.8	$6,071.7	$79,132.0	$72,417.0	$64,595.3
4	$0.0	$21.4	$973.1	$70,525.0	$3,958.8	$644.6	$37.8	$6,071.7	$82,232.4	$73,062.4	$62,734.7
5	$0.0	$21.4	$973.1	$71,157.2	$1,359.2	$644.6	$37.8	$6,071.7	$80,265.1	$69,237.4	$57,227.9
6	$0.0	$21.4	$973.1	$71,801.1	$3,958.8	$644.6	$37.8	$6,071.7	$83,508.6	$69,937.1	$55,645.3
7	$0.0	$21.4	$973.1	$72,457.0	$1,359.2	$644.6	$37.8	$6,071.7	$81,564.9	$66,319.7	$50,794.5
8	$0.0	$21.4	$973.1	$73,125.3	$3,958.8	$644.6	$37.8	$6,071.7	$84,832.8	$66,967.8	$49,373.5
9	$0.0	$21.4	$973.1	$73,806.0	$1,359.2	$644.6	$37.8	$6,071.7	$82,913.9	$63,546.6	$45,099.7
10	$0.0	$21.4	$973.1	$74,499.5	$3,958.8	$644.6	$37.8	$6,071.7	$86,207.0	$64,146.1	$43,823.3
Total	**$911.6**	**$229.6**	**$9,731.4**	**$721,596.4**	**$26,590.3**	**$6,446.0**	**$378.4**	**$61,531.4**	**$827,415.1**	**$705,241.5**	**$580,183.2**
Annualized										**$82,675.8**	**$82,605.0**
% of Total	0.1%	0.0%	1.2%	87.2%	3.2%	0.8%	0.0%	7.4%	100.0%		

Note: Totals may not add due to rounding.

3.5 TSA

This section details the costs to TSA associated with the creation and maintenance of a CRM Program for the surface transportation covered entities as detailed in the proposed rule. These costs include the costs for TSA to review and/or approve a cybersecurity evaluation (CSE), Cybersecurity Operational Implementation Plan (COIP), CIRP, and a Cybersecurity Assessment Plan (CAP) for the covered owner/operators. Additionally, Sections § 1586.103 and 1586.105 add additional requirements related to the physical security portion of the pipeline security program. TSA would also incur costs related to the implementation of these physical security requirements.

3.5.1 Physical Security Incident Reporting Cost

Under the proposed rule, each pipeline entity is required to report any potential threats and significant physical security concerns involving transportation-related operations to TSA. TSA would incur time to engage in phone calls and record information related to the physical security incidents reported by pipeline entities.

TSA estimates an average of 25.29 calls would be made per entity per year to report such incidents.[355] TSA therefore multiplies the average calls per entity (25.29) by the total number of entities (115) to estimate a total of 2,908.35 incidents reported annually. TSA estimates a time burden of 0.32 hours per phone call made up of 0.05 hours to engage in phone calls, 0.0167 hours to record necessary information, and 0.25 hours to evaluate incident reports.[356]

---

[355] Internal TSA data suggests 101.14 calls per entity per year however, however, given uncertainty in the number of pipeline physical security incidents, TSA applies a 75 percent reduction from this value for a total of 25.29 incidents per entity per year.

[356] TSA data from the Transportation Security Operations Center (TSOC) shows that the average phone call is approximately 3 minutes (0.05 hours) in duration.

TSA uses the blended I-Band and J-Band wage rate of $80.54 per hour as discussed in Section 2.3.6. TSA then multiplies the blended compensation rate ($80.54) by the number of incidents (2,908) and the reporting time burden (0.32 hours) to calculate the cost to TSA of pipeline physical security incident reporting as presented in Table 3-81.

Table 3-81: TSA Pipeline Physical Security Incident Reporting Cost ($ Thousands)

Year	Pipeline Population	Number of Incidents	TSA Pipeline Physical Security Incident Reporting Cost
	a = Column j, Table 2-1	b = a × 25.29	c = b × 0.32 hours × $80.54
1	115.00	2,908.35	$75.0
2	115.00	2,908.35	$75.0
3	115.00	2,908.35	$75.0
4	115.00	2,908.35	$75.0
5	115.00	2,908.35	$75.0
6	115.00	2,908.35	$75.0
7	115.00	2,908.35	$75.0
8	115.00	2,908.35	$75.0
9	115.00	2,908.35	$75.0
10	115.00	2,908.35	$75.0
Total			$749.6

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

3.5.2 Cybersecurity Evaluations (CSE) Cost

Under the proposed rule, each owner/operator is required to complete an initial and recurrent cybersecurity evaluation that must be submitted to TSA. TSA estimates it would incur four hours to process each entity's evaluation each year as discussed in Section 2.4.3.

TSA uses the blended I-Band and J-Band wage rate of $80.54 per hour as discussed in Section 2.3.6. TSA then multiplies the blended compensation rate ($80.54) by the number of evaluations submitted in each mode and the time burden to process each evaluation (4 hours) to calculate the cost to TSA of cybersecurity evaluation processing as presented in Table 3-82.[357]

[357] See Section 2.4.3 for the estimated number of CSE submissions for each mode.

Table 3-82: TSA Cost to Process Cybersecurity Evaluations (CSE) ($ Thousands)

Year	Cybersecurity Evaluations (CSE) Submitted			Total CSEs	TSA CSE Review Cost
	Pipelines	Freight Rail	PTPR		
	a = Column j, Table 2-1	b = Column a, Table 2-1	c = Column d, Table 2-1	d = ∑a,b,c	e = d × 4 hours × $80.54
1	115.00	73.00	34.00	222.00	$71.5
2	115.00	73.57	34.74	223.31	$71.9
3	115.00	74.14	35.51	224.65	$72.4
4	115.00	74.72	36.28	226.00	$72.8
5	115.00	75.31	37.08	227.39	$73.3
6	115.00	75.90	37.89	228.79	$73.7
7	115.00	76.49	38.72	230.21	$74.2
8	115.00	77.09	39.57	231.66	$74.6
9	115.00	77.69	40.43	233.12	$75.1
10	115.00	78.30	41.32	234.62	$75.6
Total					**$735.1**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

3.5.3 Cybersecurity Operational Implementation Plans (COIP) Cost

As detailed in § 1580.307, 1582.207, and 1586.207, all owner/operators must adopt a COIP and submit the plan to TSA, who would later notify the owner/operator's accountable executive of approval. As discussed in Section 2.4.3, TSA estimates a time burden of 50 hours to review and approve each entity's COIP in Year 1. TSA SMEs with surface operations expertise estimate the 50 hours includes three J-Band level employees each spending 14 hours reviewing the COIP, as well as two K-Band level employees each spend four hours on review. For years 2-10, TSA estimates a time burden of 50 hours, in any one year in a three-year period, presented as an annual average of 16.67 hours.

TSA calculates a weighted compensation rate of $89.52 per hour using the wage rate of $87.11 for J-Band employees and of $102.20 for K-Band employees.[358] TSA then multiplies the weighted compensation rate ($89.52) by the COIP review time burden (50 hours) and number of

[358] The weighted compensation rate is calculated as ($87.11 × 3 × 14 hours) + ($102.20 × 2 × 4 hours) ÷ 50 hours. Value used in analysis is rounded to two decimal places.

affected pipeline, freight rail, and PTPR entities per year to calculate the cost to TSA to process COIPs.

TSA also assumes 50 percent of submitted COIPs would require TSA legal review. As discussed in Section 2.4.4, TSA SMEs with surface operations expertise estimates legal review would require four hours at a K-Band employee level. TSA multiplies the K-Band wage rate of $102.20 per hour, as described in Section 2.3.6, by the COIP legal review time burden (4 hours) and number of COIPs requiring legal review per year to calculate the cost to TSA for legal review of COIPs.

Table 3-83 presents the total cost of TSA COIP review over 10 years. It includes TSA COIP review and COIP legal review costs.

Table 3-83: TSA Cybersecurity Operational Implementation Plans (COIP) Review Cost ($ Thousands)

Year	COIPs Submitted			Total COIPs	TSA COIP Review Cost	TSA COIP Legal Review	Total TSA COIP Review Cost
	Pipelines	Freight Rail	PTPR				
	a = Column j, Table 2-1	b = Column a, Table 2-1	c = Column d, Table 2-1	d = ∑a,b,c	e_{y1} = d × 50 hours × $89.52 e_{yn} = d x 16.67 hours x $89.52	f = d × 0.5 × 4 hours × $102.20	g = e + f
1	115.00	73.00	34.00	222.00	$993.7	$45.4	$1,039.1
2	-	0.57	0.74	1.31	$2.0	$0.3	$2.2
3	-	0.57	0.77	1.34	$2.0	$0.3	$2.3
4	-	0.58	0.77	1.35	$2.0	$0.3	$2.3
5	-	0.59	0.80	1.39	$2.1	$0.3	$2.4
6	-	0.59	0.81	1.40	$2.1	$0.3	$2.4
7	-	0.59	0.83	1.42	$2.1	$0.3	$2.4
8	-	0.60	0.85	1.45	$2.2	$0.3	$2.5
9	-	0.60	0.86	1.46	$2.2	$0.3	$2.5
10	-	0.61	0.89	1.50	$2.2	$0.3	$2.5
Total					**$1,012.6**	**$48.0**	**$1,060.5**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

In addition, TSA would engage in COIP related training to ensure employees are able to effectively evaluate each entity's COIP. A TSA SME with surface operations expertise estimates 100 J-Band level employees would spend 40 hours each quarter, for a total of 160 hours per year, on COIP related training in Years 1 through 3 of the rule. Beginning in Year 4, TSA estimates the time burden of this training would decrease to 40 hours annually and continue through Year 10.

In addition to time spend undergoing such training, as discussed in Section 2.4.4, a TSA SME with surface operations expertise estimates five J-band level employees would each spend 100 hours in Year 1 to develop the training program for a total of 500 hours. TSA estimates that in Years 2 and 3 of this rule the time burden would decrease to 50 hours per person, for a total of 250 hours, and that in Years 4 through 10 the time burden would further decrease to 20 hours per person, for a total of 100 hours.

TSA uses the wage rate of $87.11 for J-Band level employees (see Section 2.3.6) to calculate all costs associated with COIP related training. TSA first multiplies the wage rate ($87.11) by the time burden to engaged in training (160 hours in Years 1 through 3, 40 hours in Years 4 through 10) and the number of individuals engaged in training (100) to calculate the cost of training engagement. TSA then multiplies the wage rate ($87.11) by the time burden to develop training (500 hours in Year 1, 250 hours in Years 2 and 3, and 100 hours in Years 4 through 10) to calculate the cost to TSA of training development as presented in Table 3-84.

Table 3-84: TSA Cost of COIP Related Training ($ Thousands)

Year	TSA Employee Population	TSA Training Time	TSA Training Cost	TSA Time to Develop Training	TSA Training Development Cost	TSA Total Training Cost
	a	b	c = a × b × $87.11	d	e = d × $87.11	f = c + e
1	100	160	$1,393.8	500	$43.6	$1,437.3
2	100	160	$1,393.8	250	$21.8	$1,415.5
3	100	160	$1,393.8	250	$21.8	$1,415.5
4	100	40	$348.4	100	$8.7	$357.2
5	100	40	$348.4	100	$8.7	$357.2
6	100	40	$348.4	100	$8.7	$357.2
7	100	40	$348.4	100	$8.7	$357.2
8	100	40	$348.4	100	$8.7	$357.2
9	100	40	$348.4	100	$8.7	$357.2
10	100	40	$348.4	100	$8.7	$357.2
Total						**$6,768.4**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

3.5.3.1 Governance of the CRM Program Cost

Under the proposed rule, all owner/operators are required to provide to TSA the name, titles, business numbers, and business email addresses of the owner/operator's accountable executive. As discussed previously in Section 2.4.4.1, TSA estimates that each entity would designate one individual to fulfill this role.

Based on its experience with processing other similar roles (e.g., physical security coordinators) TSA estimates a time burden of five hours per designated accountable executive to process the information provided by the owner/operator. TSA uses the blended I-Band and J-Band wage rate of $80.54 per hour as discussed in Section 2.3.6. TSA then multiplies the blended compensation rate ($80.54) by the number of accountable executives in each mode and time burden to process their information (5 hours) to calculate the cost to TSA to process accountable executive information as presented in Table 3-85.

Table 3-85: TSA Cost to Process Accountable Executive Information ($ Thousands)

Year	Accountable Executives			Total Accountable Executives	Total Cost to Record Information
	Pipelines	Freight Rail	PTPR		
	a = Table 3-58	b = Table 3-3	c = Table 3-28	d = a + b + c	e = d x 5 hours x $80.54
1	115.00	73.00	34.00	222.00	$89.4
2	15.72	3.51	5.24	24.47	$9.9
3	15.72	3.55	5.37	24.64	$9.9
4	15.72	3.57	5.47	24.76	$10.0
5	15.72	3.61	5.61	24.94	$10.0
6	15.72	3.64	5.72	25.08	$10.1
7	15.72	3.65	5.85	25.22	$10.2
8	15.72	3.69	5.98	25.39	$10.2
9	15.72	3.71	6.10	25.53	$10.3
10	15.72	3.74	6.25	25.71	$10.4
Total					$180.3

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

3.5.3.2 Cybersecurity Coordinator Cost

Under the proposed rule, all owner/operators are required to designate a primary and at least one alternate cybersecurity coordinator to serve as the primary contact for cyber-related intelligence information and activities and communications with TSA and CISA. Owner/operators must provide to TSA the names, titles, business numbers, and business email addresses of the cybersecurity coordinator and alternate(s). As discussed previously in Section 2.4.4.2, TSA estimates that all entities would designate one primary coordinator and one alternate for a total of two individuals.

TSA estimates a time burden of 1 hour per designated individual to process the information provided by the owner/operator. TSA uses the blended I-Band and J-Band wage rate of $80.54 per hour as discussed in Section 2.3.6. TSA then multiplies the blended compensation rate ($80.54) by the number of cybersecurity coordinators in each mode and time burden to process their information (1 hour) to calculate the cost to TSA to process cybersecurity coordinator information as presented in Table 3-86.

Table 3-86: TSA Cost to Process Cybersecurity Coordinator Information ($ Thousands)

Year	Cybersecurity Coordinator and Alternate Populations			Total Cybersecurity Coordinators	Total Cost to Record Information
	Pipelines	Freight Rail	PTPR		
	a = Column d, Table 3-60	b = Column d, Table 3-5	c = Column d, Table 3-30	d = a + b + c	e = d x 1 hour x $80.54
1	230.00	146.00	68.00	444.00	$35.8
2	31.44	7.03	10.48	48.95	$3.9
3	31.44	7.07	10.74	49.25	$4.0
4	31.44	7.14	10.94	49.52	$4.0
5	31.44	7.20	11.21	49.85	$4.0
6	31.44	7.25	11.44	50.13	$4.0
7	31.44	7.30	11.70	50.44	$4.1
8	31.44	7.37	11.96	50.77	$4.1
9	31.44	7.42	12.20	51.06	$4.1
10	31.44	7.48	12.49	51.41	$4.1
Total					**$72.1**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

3.5.3.3 Cybersecurity Training Cost

Under the proposed rule, all owner/operators are required to submit a cybersecurity training plan to TSA for approval. TSA anticipates each entity would submit a training plan to TSA in Year 1 and that this process would include some discussion with TSA on modifications needed.[359] TSA assumes the level of effort to review cybersecurity training plans is similar to the effort to review security training plans which TSA estimates as 40 hours to review and approve initial training plan submissions.[360] TSA uses the blended I-Band and J-Band wage rate of $80.54 per hour as discussed in Section 2.3.6. TSA multiplies the blended compensation rate ($80.54) by the number of initial training plan submissions in each mode and time burden to process each submission (40 hours) to calculate the cost to TSA to process training plan submissions.

[359] Owners/operators required to have a Cybersecurity training program would have to submit a plan within 90 days of the effective date of the final rule.

[360] See "Security Training Programs for Surface Transportation Employees – Final Rulemaking." RIN: 1652-AA55. Regulatory Impact Analysis. Page 93.

Table 3-87: TSA Cost to Process Cybersecurity Training Plans ($ Thousands)

Year	Cybersecurity Training Plans				Total Cost
	Pipelines	Freight Rail	PTPR	Total Plans Submitted	
	a = Column k, Table 2-1	b = Column b, Table 2-1	c = Column e, Table 2-1	d = a + b + c	e = d x 40 hours x $80.54
1	115.00	73.00	34.00	222.00	$715.20
2	-	0.57	0.74	1.31	$4.22
3	-	0.57	0.77	1.34	$4.32
4	-	0.58	0.77	1.35	$4.35
5	-	0.59	0.80	1.39	$4.48
6	-	0.59	0.81	1.40	$4.51
7	-	0.59	0.83	1.42	$4.57
8	-	0.60	0.85	1.45	$4.67
9	-	0.60	0.86	1.46	$4.70
10	-	0.61	0.89	1.50	$4.83
Total					**$755.9**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

TSA would also incur a cost to inspect training records for each employee that undergoes the required cybersecurity training, including records of both basic cybersecurity training and role-based cybersecurity training. TSA calculates the number of training records by industry type with inputs from, Table 3-14, Table 3-39, and Table 3-69. TSA estimates it would take four hours of time to inspect each entities' training records and uses a wage rate of $56.80 for the H-Band employee level who would incur this time as presented in Table 2-9.

TSA calculates the cost of inspecting training records by multiplying the H-Band wage rate ($53.96) by the cybersecurity training records hour burden (4 hours) and the number of regulated entities in each mode to present a cybersecurity training records inspection cost in Table 3-88 below.

Table 3-88: TSA Cost to Inspect Cyber Training Records

Year	Training Records Inspections			Total Records Submitted	Total TSA Training Record Inspection Cost
	Pipelines	Freight Rail	PTPR		
	a = Column j, Table 2-1	b = Column a, Table 2-1	c = Column d, Table 2-1	d = ∑a,b,c	e = d x 4 hours x $53.96
1	115.00	73.00	34.00	222.00	$47.9
2	115.00	73.57	34.74	223.31	$48.2
3	115.00	74.14	35.51	224.65	$48.5
4	115.00	74.72	36.28	226.00	$48.8
5	115.00	75.31	37.08	227.39	$49.1
6	115.00	75.90	37.89	228.79	$49.4
7	115.00	76.49	38.72	230.21	$49.7
8	115.00	77.09	39.57	231.66	$50.0
9	115.00	77.69	40.43	233.12	$50.3
10	115.00	78.30	41.32	234.62	$50.6
Total					**$492.5**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

TSA would also spend time in Year 1 to train TSIs to inspect new programs. TSA estimates 220 TSIs would undergo this training and that the training would take four hours to complete.[361] TSA uses the blended I-Band and J-Band wage rate of $80.54 per hour as discussed in Section 2.3.6.

TSA calculates a cost to train TSIs to inspect regulated entities according to the new program as the inspector wage rate ($80.54) multiplied by the training inspection hour burden (4 hours) and the number of TSIs requiring the new training. This cost would only occur in the first year and equates to $70.9 thousand.[362]

3.5.4 Cybersecurity Incident Response Plan (CIRP) Cost

Under the proposed rule, each owner/operator must submit a CIRP to TSA in Year 1. TSA estimates it would incur a time burden of four hours to process each CIRP. TSA uses the blended I-Band and J-Band wage rate of $80.54 per hour as discussed in Section 2.3.6. TSA then multiplies the blended compensation rate ($80.54) by the number of CIRPs submitted in each

[361] TSA estimates it would require a half day of training for TSIs to learn the new inspection guidelines.
[362] TSA calculates the TSI training cost as $80.54/hr. × 4 hours × 220 = $70,875.

mode and time burden to process each CIRP (4 hours) to calculate the cost to TSA to process CIRPs as presented in Table 3-89.

Table 3-89: TSA Cost to Process Cybersecurity Incident Response Plans (CIRP) ($ Thousands)

Year	Cybersecurity Incident Response Plans (CIRP)			Total CIRPs Submitted	Total TSA CIRP Review Cost
	Pipelines	Freight Rail	PTPR		
	a = Column k, Table 2-1	b = Column b, Table 2-1	c = Column e, Table 2-1	d = ∑a,b,c	e = d × 4 hours x $80.54
1	115.00	73.00	34.00	222.00	$71.5
2	-	0.57	0.74	1.31	$0.4
3	-	0.57	0.77	1.34	$0.4
4	-	0.58	0.77	1.35	$0.4
5	-	0.59	0.80	1.39	$0.4
6	-	0.59	0.81	1.40	$0.5
7	-	0.59	0.83	1.42	$0.5
8	-	0.60	0.85	1.45	$0.5
9	-	0.60	0.86	1.46	$0.5
10	-	0.61	0.89	1.50	$0.5
Total					$75.6

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

TSA would also incur time to respond to any identified cybersecurity incidents. TSA estimates that 10 percent of all reported cybersecurity incidents would require TSA personnel on-site each year. As discussed in Section 2.4.6, TSA estimates responding to cybersecurity incidents would require 32 hours of on-site personnel time per incident. TSA uses the blended I-Band and J-Band wage rate of $80.54 per hour as discussed in Section 2.3.6.

TSA calculates the agency cost to respond on-site to cybersecurity incidents by multiplying the I/J-Band blended wage ($80.54) by the on-site response time hour burden (32 hours) and the expected volume of cybersecurity incidents per regulated mode.

TSA also estimates the cost of travel associated with responding to cybersecurity incidents on-site. As discussed in Section 2.4.6, TSA estimates the total travel related costs as $2,144 per incident which includes lodging, per diem, and transportation.

TSA calculates the cost of travel for agency personnel as the sum of the meals, incidental

expenses, as well as flights and lodging expenses ($2,144) which are then multiplied by the sum of expected incidents for all regulated modes. TSA presents the cost of travel for agency personnel over 10 years in Table 3-90 below.

TSA presents the costs calculated for incident response time on-site below in Table 3-90.

Table 3-90: TSA Cost to Respond to Cybersecurity Incidents ($ Thousands)

Year	Cybersecurity Incidents			Total Incidents with Onsite Response	Total Onsite Incident Response Cost	Total Travel Cost	Total TSA Response Cost
	Pipelines	Freight Rail	PTPR				
	a = Column b, Table 3-73 × 10%	b = Column b, Table 3-18 × 10%	c = Column b, Table 3-43 × 10%	d = a + b + c	e = d × 32 hours × $80.54	f = d × $2,144	g = e + f
1	40.02	1.02	1.50	42.54	$109.6	$91.1	$200.7
2	40.02	1.03	1.53	42.58	$109.7	$91.1	$200.8
3	40.02	1.04	1.56	42.62	$109.8	$91.1	$200.9
4	40.02	1.05	1.60	42.66	$110.0	$91.1	$201.1
5	40.02	1.05	1.63	42.71	$110.1	$91.1	$201.2
6	40.02	1.06	1.67	42.75	$110.2	$91.1	$201.3
7	40.02	1.07	1.70	42.79	$110.3	$91.1	$201.4
8	40.02	1.08	1.74	42.84	$110.4	$91.1	$201.5
9	40.02	1.09	1.78	42.89	$110.5	$91.1	$201.6
10	40.02	1.10	1.82	42.93	$110.7	$91.1	$201.8
Total							**$2,012.3**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

3.5.5 Cybersecurity Assessment Plan (CAP) Cost

Under the proposed rule, all owner/operators must submit a Cybersecurity Assessment Plan (CAP) to TSA for review and approval each year. As discussed in Section 2.4.7, a TSA SME with cybersecurity expertise estimates a time burden of 32 hours to review each entity's CAP each year. TSA uses the blended I-Band and J-Band wage rate of $80.54 per hour as discussed in Section 2.3.6. TSA then multiplies the blended compensation rate ($80.54) by the number of entities in each mode and the time burden to review each CAP (32 hours) to calculate the cost to TSA to process CAPs as presented in Table 3-91.

Table 3-91: TSA Cost to Process Cybersecurity Assessment Plans (CAP) ($ Thousands)

Year	Cybersecurity Assessment Plans (CAPs)			Hour Burden	Total Cost
	Pipelines	Freight Rail	PTPR		
	a = Column j, Table 2-1	b = Column a, Table 2-1	c = Column d, Table 2-1	d = ∑a,b,c	e = d x 32 hours x $80.54
1	115.00	73.00	34.00	222.00	$572.2
2	115.00	73.57	34.74	223.31	$575.5
3	115.00	74.14	35.51	224.65	$579.0
4	115.00	74.72	36.28	226.00	$582.5
5	115.00	75.31	37.08	227.39	$586.0
6	115.00	75.90	37.89	228.79	$589.7
7	115.00	76.49	38.72	230.21	$593.3
8	115.00	77.09	39.57	231.66	$597.1
9	115.00	77.69	40.43	233.12	$600.8
10	115.00	78.30	41.32	234.62	$604.7
Total					**$5,880.7**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

3.5.6 Total Cost Impact to TSA

The total cost impact for all requirements for TSA is $18.9 million undiscounted over 10 years, $16.6 million discounted at 3 percent, and $14.2 million discounted at 7 percent. TSA aggregates the costs of Physical Security, the CRM Program, and the CIRP in Table 3-92 below.

Table 3-92: Summary of Proposed Rule Requirement Costs - TSA ($ Thousands)

Year	Physical Security Costs	CRM Program			CIRP	Total Costs		
		CSE	COIP	CAP		f = ∑a,b,c,d,e		
	a	b	c	d	e	Undiscounted	Discounted at 3%	Discounted at 7%
1	$75.0	$71.5	$3,435.6	$572.2	$272.3	$4,426.4	$4,297.5	$4,136.9
2	$75.0	$71.9	$1,484.0	$575.5	$201.3	$2,407.7	$2,269.5	$2,102.9
3	$75.0	$72.4	$1,484.5	$579.0	$201.4	$2,412.2	$2,207.5	$1,969.1
4	$75.0	$72.8	$426.5	$582.5	$201.5	$1,358.2	$1,206.8	$1,036.2
5	$75.0	$73.3	$427.1	$586.0	$201.6	$1,363.0	$1,175.7	$971.8
6	$75.0	$73.7	$427.6	$589.7	$201.7	$1,367.6	$1,145.3	$911.3
7	$75.0	$74.2	$428.0	$593.3	$201.8	$1,372.3	$1,115.8	$854.6
8	$75.0	$74.6	$428.6	$597.1	$202.0	$1,377.2	$1,087.2	$801.6
9	$75.0	$75.1	$429.0	$600.8	$202.1	$1,382.0	$1,059.2	$751.7
10	$75.0	$75.6	$429.7	$604.7	$202.2	$1,387.1	$1,032.1	$705.1
Total	**$749.6**	**$735.1**	**$9,400.6**	**$5,880.7**	**$2,087.9**	**$18,853.8**	**$16,596.7**	**$14,241.2**
Annualized							**$1,945.6**	**$2,027.6**

Note: Totals may not add due to rounding.

3.6 Total Cost of the Proposed Rule

TSA estimates the total cost of the proposed rule by summing the total costs to the four regulated industries plus TSA (See Table 3-25, Table 3-50, Table 3-53, Table 3-80, and Table 3-92). The total cost of the proposed rule aggregates to $3,089.8 million undiscounted over ten years, $2,631.0 million discounted at 3 percent, and $2,161.6 million discounted at 7 percent. As previously discussed, TSA estimates the full costs of the CRM program without adjusting for costs industry has incurred as a result of the SDs but does provide a comparison of costs associated with the SDs in Section 3.7. TSA also provides a sensitivity analysis in Section 3.8 which assesses uncertainty of key cost drivers which includes aspects of existing compliance as well. Nonetheless, individual owner/operators may still experience higher and lower costs than the average impacts used in the analysis, especially due to the performance based nature of the requirements. In addition, there are some areas or impacts of the rule where costs have not been quantified. Such unquantified costs include actual mitigation measures implemented as a result of the rule but not otherwise captured, additional administrative costs incurred throughout the implementation process beyond what TSA has already estimated, as well as the costs incurred as a result of the COIP amendment process. TSA also does not quantify potential new position or hiring costs but acknowledges that owner/operators may incur such costs if additional personnel are needed to comply with the requirements of the proposed rule.

Under the proposed rule, regulated industries would incur a total cost of $3,071.0 million undiscounted over ten years. Table 3-93 summarizes the total cost of the proposed rule by regulated industries.

Table 3-93: 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	$97,652.0	$119,996.3	$188.5	$85,636.2	$303,473
2	$95,471.4	$120,633.3	$6.0	$81,122.2	$297,233
3	$94,622.4	$121,507.8	$6.1	$79,132.0	$295,268
4	$97,002.7	$123,882.8	$6.3	$82,232.4	$303,124
5	$96,187.3	$124,813.9	$6.4	$80,265.1	$301,273
6	$98,675.1	$127,288.7	$6.6	$83,508.6	$309,479
7	$97,885.3	$128,279.4	$6.8	$81,564.9	$307,736
8	$100,405.1	$130,820.6	$6.9	$84,832.8	$316,065
9	$99,647.7	$131,873.8	$7.1	$82,913.9	$314,442
10	$102,200.5	$134,484.0	$7.3	$86,207.0	$322,899
Total	**$979,749.6**	**$1,263,580.7**	**$247.9**	**$827,415.1**	**$3,070,993.4**

Note: Totals may not add due to rounding.

TSA would also incur a total cost of $18.9 million undiscounted over ten years. However, the cost to regulated industries makes up the vast majority of proposed rule costs compared to TSA. Among the regulated industries, freight rail, PTPR, OTRB, and pipelines account for approximately 31.9 percent, 41.1 percent, less than 0.01 percent, and 26.9 percent respectively of the overall cost of the rule. Table 3-94 presents the total cost of the proposed rule.

Table 3-94: Total Cost of the Proposed Rule ($ Thousands)

Year	Total Regulated Industries Cost	TSA Cost	Total Proposed Rule Cost		
			c = a + b		
	a	b	Undiscounted	Discounted at 3%	Discounted at 7%
1	$303,473.1	$4,426.4	$307,899.5	$298,931.5	$287,756.5
2	$297,232.9	$2,407.7	$299,640.5	$282,439.9	$261,717.6
3	$295,268.4	$2,412.2	$297,680.6	$272,419.9	$242,996.0
4	$303,124.3	$1,358.2	$304,482.5	$270,528.8	$232,288.2
5	$301,272.8	$1,363.0	$302,635.8	$261,056.3	$215,775.1
6	$309,479.0	$1,367.6	$310,846.6	$260,329.1	$207,130.2
7	$307,736.3	$1,372.3	$309,108.6	$251,333.6	$192,497.3
8	$316,065.4	$1,377.2	$317,442.6	$250,592.2	$184,754.5
9	$314,442.5	$1,382.0	$315,824.5	$242,053.2	$171,787.6
10	$322,898.8	$1,387.1	$324,285.9	$241,299.2	$164,850.5
Total	**$3,070,993.4**	**$18,853.8**	**$3,089,847.2**	**$2,630,983.7**	**$2,161,553.8**
Annualized				**$308,431.6**	**$307,756.6**

Note: Totals may not add due to rounding.

Table 3-95 shows the cost to regulated industries by requirement, while Table 3-96 shows the Costs by CFR Part. The CRM Program is the largest cost, making up over 99 percent of the total

cost to regulated entities.

Table 3-95: Total Undiscounted Costs by Requirement - Regulated Industries ($ Thousands)

Year	Familiarization	CRM Program				Reporting Cybersecurity Incidents	CIRP	Physical Security	Total Cost
		CSE	COIP	CAP	Recordkeeping and Compliance				
	a	b	c	d	e	f	g	h	i = ∑a,b,c,d,e,f,g,h
1	$1,395.6	$1,310	$287,360	$2,603	$1,005	$41.4	$9,721.0	$37.0	$303,473.1
2	$7.8	$1,314	$279,035	$7,636	$1,009	$41.4	$8,167.9	$21.4	$297,232.9
3	$8.0	$1,318	$282,009	$2,663	$1,013	$41.5	$8,193.9	$21.4	$295,268.4
4	$8.1	$1,322	$284,796	$7,697	$1,017	$41.6	$8,220.0	$21.4	$303,124.3
5	$8.3	$1,326	$287,881	$2,726	$1,022	$41.6	$8,247.1	$21.4	$301,272.8
6	$8.5	$1,331	$291,016	$7,761	$1,026	$41.7	$8,274.1	$21.4	$309,479.0
7	$8.7	$1,335	$294,208	$2,790	$1,030	$41.8	$8,301.6	$21.4	$307,736.3
8	$8.8	$1,340	$297,463	$7,826	$1,035	$41.9	$8,329.8	$21.4	$316,065.4
9	$9.0	$1,344	$300,773	$2,856	$1,039	$41.9	$8,358.0	$21.4	$314,442.5
10	$9.2	$1,349	$304,153	$7,893	$1,043	$42.0	$8,387.2	$21.4	$322,898.8
Total	**$1,472.1**	**$13,288**	**$2,908,694**	**$52,452**	**$10,240**	**$416.8**	**$84,200.7**	**$229.6**	**$3,070,993.4**

Note: Totals may not add due to rounding.

Table 3-96: Cost by CFR Part (Discounted at 7 Percent, $ Thousands)

49 CFR Part	Affected Industry	Requirements/Burden	Specifically Required by Statute?[363]	Ten-Year Cost to Industry or TSA ($ Thousands)
1580 – Freight Rail Transportation Security				
§ 1580.101 Scope	Freight Rail	Provision 101 adds a scope to Part 1580 for the proposed rule.	No	Not Quantified/Procedural
§ 1580.301 Scope and applicability	Freight Rail	Adding a scope to proposed part 1580 subpart D and clarifying which entities would be covered by the applicability of the proposed rule based on TSA's exercise of its discretion. Includes costs associated with determining applicability and entity familiarization with the rule.	No	**Freight Rail: $238.6**
§ 1580.303 Form, content, and availability of Cybersecurity Risk Management program	Freight Rail	Adding proposed § 1580.303, which describes the form that a CRM program should take in addition to its content and the availability to access said program information.	No	Not Quantified/Procedural. Costs for CRM Program elements are captured in individual CFR Sections.
§ 1580.305 Cybersecurity evaluation	Freight Rail	Under proposed § 1580.305 covered entities must assess their cybersecurity systems annually and notify TSA within seven days of completing said assessments in addition to making assessments available to TSA. While a cybersecurity evaluation is not expressly required by statute, 6 USC 1162(a)(1)(A), 6 USC 1162(d)(1)(A), (B), (C) and (D), stipulate that for railroad carriers assigned to a high-risk tier, the Secretary requires a vulnerability assessment to identify and evaluate critical railroad carrier assets and infrastructure, identify vulnerabilities to those assets and infrastructure, and identify redundant and back-up systems. Furthermore, 6 USC 1162(k) requires that no later than 3 years after the date on which the vulnerability assessment or security plan is approved, and at least five years thereafter, railroad carriers still assigned to a high-risk tier	No	Freight Rail: $1,689.3 TSA: $170.4 **Total: $1,859.6**

[363] For purposes of this document, we use "specifically required by statute" to denote only those provisions explicitly referenced in statute that must be implemented without any discretion as to the scope of the requirements or the means of implementation, as they relate to the requirements contained in the proposed rule. This table does not reflect a conclusive view of the agency as to the scope of statutory mandates or the relationship between such mandates and the proposed rule. TSA welcomes comments on the table and on the subject matter more broadly.

49 CFR Part	Affected Industry	Requirements/Burden	Specifically Required by Statute?[363]	Ten-Year Cost to Industry or TSA ($ Thousands)
		must submit an evaluation of the adequacy of the vulnerability assessment and include any material changes made.		
§ 1580.307 Cybersecurity Operational Implementation Plan	Freight Rail	Under proposed § 1580.307, covered entities would be required to include their defense plans, physical and logical/virtual security controls, and compliance with other sections of this rule within their COIPs.	No	Specific cost elements of the COIP are included under §1580.309, §1580.311, §1580.313, §1580.315, and §1580.317.
§ 1580.309 Governance of the CRM program	Freight Rail	Under proposed § 1580.309, covered entities would be required to identify and designate an accountable executive for the CRM program. This individual's contact and identifying information must be provided to TSA and incorporated into the COIP. The cost of this provision also includes time to create and maintain the COIP.	No	Freight Rail: $1,391.2 TSA: $2,106.6 **Total: $3,497.8**
§ 1580.311 Cybersecurity Coordinator	Freight Rail	Under proposed § 1580.311, covered entities would be required to identify and designate a primary and at least one alternate cybersecurity coordinator who is accessible to TSA 24 hours a day seven days a week. The name, title, phone numbers, and email addresses of the coordinators and their alternatives must be given to TSA. The proposed § 1580.311 also requires that the primary security coordinator and alternate be U.S. citizens eligible for a security clearance, unless otherwise waived by TSA. While cybersecurity coordinators are not expressly required by statute, 6 USC 1162(e)(1)(A) requires railroad carriers assigned to a high-risk tier to identify a security coordinator having authority to (i) implement security actions under the plan; (ii) coordinate security improvements; and (iii) receive immediate communications from appropriate Federal officials regarding railroad security. 6 USC 1162(e)(2) expressly requires that individual serving as security coordinator is a citizen of the United States.	No	Freight Rail: $46.4 TSA: $14.5 **Total: $61.0**
§ 1580.313 Identification of Critical Cyber Systems	Freight Rail	Under proposed § 1580.313, covered entities would be required to identify critical cyber systems, including both OT and IT systems. These systems will need to be incorporated into the COIP and include specific identifying information for the system in addition to the manufacturer or designer for each system.	Partially. 6 USC 1162(a)(1)(A), 6 USC 1162(d)(1)(A) and (D), and 6 USC 1162(k) stipulate that for railroad carriers assigned to a high-risk tier, the Secretary require a periodic vulnerability	**Freight Rail: $2,878.1**

49 CFR Part	Affected Industry	Requirements/Burden	Specifically Required by Statute?[363]	Ten-Year Cost to Industry or TSA ($ Thousands)
			assessment to identify and evaluate critical railroad carrier assets and infrastructure, which includes identification and evaluation of critical assets and infrastructure.	
§ 1580.315 Supply chain risk management	Freight Rail	Under proposed § 1580.315, covered entities would be required to incorporate supply chain incident reporting into their procurement documents and contracts, ensure that these documents stipulate vendors or service providers notify the procuring customer of security vulnerabilities within a risk-informed time frame, and that the documents include cybersecurity requirements and questions.	No	**Freight Rail: $17,073.0**
§ 1580.317 Protection of Critical Cyber Systems	Freight Rail	Under proposed § 1580.317, covered entities would be required to describe their network segmentation policies and controls necessary to address cybersecurity threats. This includes implementing network segmentation of critical systems, managing identification and authentication policies, implementing multi-factor authentication, implementing zero trust policies, ensuring that all critical cyber systems are up to date on patches, storing logging data in a secured and centralized system, and ensure that backups are stored in a secure manner and are free of malicious code.	Partially. 6 USC 1162(e)(1)(G) stipulates the Secretary require that each security plan of a railroad carrier assigned to a high-risk tier includes plans for providing redundant and backup systems required to ensure the continued operation of critical elements of the railroad carrier's system in the event of a terrorist attack or other incident.	Freight Rail: $562,173.9 Freight Rail: $70,308.3 TSA: $367.2 **Total: $70,675.5**
§ 1580.319 Cybersecurity training and knowledge	Freight Rail	Under proposed § 1580.319, covered entities would be required to provide a baseline of cybersecurity training to all employees with access to the entity's IT or OT system annually and additional training to employees with roles and responsibilities for implementing the CRM program. While cybersecurity training is not expressly required by statute, 6 USC 1162(d)(1)(C)(vii), 6 USC 1162(e)(1)(E), 6 USC 1167(a) and (d) require employee training for railroad carriers assigned to a high-risk tier which includes the determination of the seriousness of any occurrence or threat and the operation and maintenance of security equipment and systems.	No	
§ 1580.321 Detection of	Freight Rail	Under proposed § 1580.321, covered entities would be required to ensure continuous monitoring and detection policies that identify	Partially. 6 USC 1162(e)(1)(C) stipulates the Secretary require	Freight Rail: $5,271.9

49 CFR Part	Affected Industry	Requirements/Burden	Specifically Required by Statute?[363]	Ten-Year Cost to Industry or TSA ($ Thousands)
cybersecurity incidents		cybersecurity incidents as they occur and automatic measures in place to mitigate the impact.	that each security plan of a railroad carrier assigned to a high-risk tier includes procedures to be implemented or used by the railroad carrier in response to a terrorist attack.	
§ 1580.323 Capabilities to respond to a cybersecurity incident	Freight Rail	Under proposed § 1580.323, covered entities would be required to implement into its COIP capabilities to respond to cybersecurity incidents affecting Critical Cyber Systems that audit unauthorized access to internet domains and addresses and document and audit any communications between the OT system and an internal or external system that deviates from the covered entities identified baseline of communication; identify and respond to execution of unauthorized code, including macro scripts; and define, prioritize, and drive standardized incident response activities, such as Security, Orchestration, Automation, and Response (SOAR).	Partially. 6 USC 1162(e)(1)(C) stipulates the Secretary require that each security plan of a railroad carrier assigned to a high-risk tier includes procedures to be implemented or used by the railroad carrier in response to a terrorist attack.	Cost captured in Reporting and Detection of Cyber Incidents
§ 1580.325 Reporting cybersecurity incidents	Freight Rail	Under proposed § 1580.325, covered entities would be required to implement incident response plans that include reporting within 24 hours to CISA and include the reporting person's name, phone number, and email progress, the location of the incident with identifying information, a description of the incident, and any additional relevant information.	No	**Freight Rail: $7.2**
§ 1580.327 Cybersecurity Incident Response Plan	Freight Rail	Under proposed § 1580.327, covered entities would be required to have a plan to ensure the impacts of incidents are limited, data backups are tested before use, isolation measures are put into place to reduce risks, and identification of who is responsible for implementing the plan. Covered entities must also conduct exercises to test the effectiveness of the plan's procedures.	Partially. 6 USC 1162(e)(1)(G) stipulates the Secretary require that each security plan of a railroad carrier assigned to a high-risk tier includes plans for providing redundant and backup systems required to ensure the continued operation of critical elements of the railroad carrier's system in the event of a terrorist attack or other incident.	Freight Rail: $10,736.1 TSA: $57.3 **Total: $10,793.4**
§ 1580.329 Cybersecurity Assessment Plan	Freight Rail	Under proposed § 1580.329, covered entities would be required to have a CAP that allowed owner/operators to conduct their own bi-annual cybersecurity design review. The CAP must include a specific schedule for assessments to ensure that at least 30 percent	No	Freight Rail: $11,960.0 TSA: $1,363.0 **Total: $13,323.0**

49 CFR Part	Affected Industry	Requirements/Burden	Specifically Required by Statute?[363]	Ten-Year Cost to Industry or TSA ($ Thousands)
		of the COIP is tested each year at a pace to ensure 100 percent is assessed over any 3-year period.		
§ 1580.331 Documentation to establish compliance	Freight Rail	Under proposed § 1580.331, covered entities would be required to, at the request of TSA, provide evidence of compliance, including copies of records if requested, sufficient to demonstrate compliance.	No	**Freight Rail: $2,002.6**
1582 - Public Transportation and Passenger Railroad Security				
§ 1582.101 Scope	PTPR	Provision 101 adds a scope to Part 1582 for the proposed rule.	No	Not Quantified/Procedural
§ 1582.201 Scope and applicability	PTPR	Adding a scope to proposed part 1582 subpart D and clarifying which entities would be covered by the applicability of the by the proposed rule based on TSA's exercise of its discretion. Includes costs associated with determining applicability and entity familiarization with the rule.	No	**PTPR: $58.8**
§ 1582.203 Form, content, and availability of Cybersecurity Risk Management program	PTPR	Adding proposed § 1582.303, which describes the form that a CRM program should take in addition to its content and the availability to access said program information.	No	Not Quantified/Procedural. Costs for CRM Program elements are captured in individual CFR Sections.
§ 1582.205 Cybersecurity evaluation	PTPR	Under proposed § 1582.205 covered entities must assess their cybersecurity systems annually and notify TSA within seven days of completing said assessments in addition to making said assessments available to TSA. While a cybersecurity evaluation is not expressly required by statute, 6 USC 1134(a) requires the Secretary to review and augment security assessments received from the Department of Transportation, and conduct additional security assessments as necessary to ensure that, at a minimum, all high risk public transportation agencies have a completed security assessment that includes identification of critical assets, infrastructure, and systems and their vulnerabilities.	No	PTPR: $791.7 TSA: $84.0 **Total: $875.7**
§ 1582.207 Cybersecurity Operational Implementation Plan	PTPR	Under proposed § 1582.207, covered entities would be required to include their defense plans, physical and logical/virtual security controls, and compliance with other sections of this rule within their COIPs.	No	Specific cost elements of the COIP are included under §1582.209, §1582.211, §1582.213,

49 CFR Part	Affected Industry	Requirements/Burden	Specifically Required by Statute?[363]	Ten-Year Cost to Industry or TSA ($ Thousands)
				§1582.215, and §1582.217.
§ 1582.209 Governance of the CRM program	PTPR	Under proposed § 1582.209, covered entities would be required to identify and designate an accountable executive for the CRM program. This individual's contact and identifying information must be provided to TSA and incorporated into the COIP.	No	PTPR: $506.5 TSA: $996.5 **Total: $1,502.9**
§ 1582.211 Cybersecurity Coordinator	PTPR	Under proposed § 1582.211, covered entities would be required to identify and designate a primary and at least one alternate Cybersecurity coordinator who is accessible to TSA 24 hours a day seven days a week. The name, title, phone numbers, and email addresses of the coordinators and their alternates must be given to TSA. The cost of this provision also includes time to create and maintain the COIP. While cybersecurity coordinators are not expressly required by statute, 6 USC 1162(e)(1)(A) requires railroad carriers assigned to a high-risk tier to identify a security coordinator having authority to (i) implement security actions under the plan; (ii) coordinate security improvements; and (iii) receive immediate communications from appropriate Federal officials regarding railroad security. 6 USC 1162(e)(2) expressly requires that individual serving as security coordinator is a citizen of the United States.	No	PTPR: $23.7 TSA: $10.7 **Total: $34.4**
§ 1582.213 Identification of Critical Cyber Systems	PTPR	Under proposed § 1582.213, covered entities would be required to identify critical cyber systems, including both OT and IT systems. These systems will need to be incorporated into the COIP and include specific identifying information for the system in addition to the manufacturer or designer for each system.	Partially for railroad carriers. 6 USC 1162(a)(1)(A), 6 USC 1162(d)(1)(A) and (D), and 6 USC 1162(k) stipulate that for railroad carriers assigned to a high-risk tier, the Secretary require a periodic vulnerability assessment to identify and evaluate critical railroad carrier assets and infrastructure, which includes identification and evaluation of critical assets and infrastructure.	**PTPR: $1,254.0**

49 CFR Part	Affected Industry	Requirements/Burden	Specifically Required by Statute?[363]	Ten-Year Cost to Industry or TSA ($ Thousands)
			Partially for public transportation. 6 USC 1134(a)(3) requires the Secretary to ensure that each completed public transportation security assessment includes identification of critical assets, infrastructure, and systems and their vulnerabilities for public transportation agencies assigned to a high-risk tier.	
§ 1582.215 Supply chain risk management	PTPR	Under proposed § 1582.215, covered entities would be required to incorporate supply chain incident reporting into their procurement documents and contracts, ensure that these documents stipulate vendors or service providers notify the procuring customer of security vulnerabilities within a risk-informed time frame, and that the documents include cybersecurity requirements and questions.	No	**PTPR: $7,241.3**
§ 1582.217 Protection of Critical Cyber Systems	PTPR	Under proposed § 1582.217, covered entities would be required to describe their network segmentation policies and controls necessary to address cybersecurity threats. This includes implementing network segmentation of critical systems, managing identification and authentication policies, implementing multi-factor authentication, implementing zero trust policies, ensuring that all critical cyber systems are up to date on patches, storing logging data in a secured and centralized system, and ensure that backups are stored in a secure manner and are free of malicious code.	Partially for railroad carriers. 6 USC 1162(e)(1)(G) stipulates the Secretary require that each security plan of a railroad carrier assigned to a high-risk tier includes plans for providing redundant and backup systems required to ensure the continued operation of critical elements of the railroad carrier's system in the event of a terrorist attack or other incident. Partially for public transportation. 6 USC 1134((c)(1)(A) stipulates that the Secretary require public transportation agencies determined by the Secretary to be high risk to develop a comprehensive security plan; 6	**PTPR: $739,466.9**

49 CFR Part	Affected Industry	Requirements/Burden	Specifically Required by Statute?[363]	Ten-Year Cost to Industry or TSA ($ Thousands)
			USC 1134(c)(2)((F) and (H) require that the Secretary ensure that security plans of high-risk public transportation agencies include plans for providing redundant and other appropriate backup systems necessary to ensure the continued operation of critical elements of the public transportation system in the event of a terrorist attack or other major incident and methods to mitigate damage within a public transportation system in case of an attack on the system, including a plan for communication and coordination with emergency responders.	
§ 1582.219 Cybersecurity training and knowledge	PTPR	Under proposed § 1582.219, covered entities would be required to provide a baseline of cybersecurity training to all employees with access to the entity's IT or OT system annually and additional training to employees with roles and responsibilities for implementing the CRM program. While cybersecurity training is not expressly required by statute, 6 USC 1162(d)(1)(C)(vii), (e)(1)(E), 6 USC 1167(a), (c)(1) and (11), and (d), 6 USC 1134(c)(2)(E), and 6 USC 1137(c)(1) and (10) address employee training for high-risk railroad carriers and public transportation agencies respectively which includes the determination of the seriousness of any occurrence or threat and the operation and maintenance of security equipment and systems.	No	PTPR: $117,549.5 TSA: $184.6 **Total: $117,734.1**
§ 1582.221 Detection of cybersecurity incidents	PTPR	Under proposed § 1582.221, covered entities would be required to ensure continuous monitoring and detection policies that identify cybersecurity incidents as they occur and automatic measures in place to mitigate the impact.	Partially for railroad carriers. 6 USC 1162(e)(1)(C) stipulates the Secretary require that each security plan of a railroad carrier assigned to a high-risk tier includes procedures to be	**PTPR: $2,536.3**

49 CFR Part	Affected Industry	Requirements/Burden	Specifically Required by Statute?[363]	Ten-Year Cost to Industry or TSA ($ Thousands)
			implemented or used by the railroad carrier in response to a terrorist attack. 6 USC 1162(e)(1)(G) stipulates the Secretary require that each security plan of a railroad carrier assigned to a high-risk tier includes plans for providing redundant and backup systems required to ensure the continued operation of critical elements of the railroad carrier's system in the event of a terrorist attack or other incident. Partially for public transportation. 6 USC 1134(c)(1)(A) stipulates that the Secretary require public transportation agencies determined by the Secretary to be high risk to develop a comprehensive security plan; 6 USC 1134(c)(2)(F) and (H) require that the Secretary ensure that security plans for high-risk public transportation agencies include plans for providing redundant and other appropriate backup systems necessary to ensure the continued operation of critical elements of the public transportation system in the event of a terrorist attack or other major incident and methods to mitigate damage within a public transportation system in case of an attack on the system,	

49 CFR Part	Affected Industry	Requirements/Burden	Specifically Required by Statute?[363]	Ten-Year Cost to Industry or TSA ($ Thousands)
			including a plan for communication and coordination with emergency responders.	
§ 1582.223 Capabilities to respond to a cybersecurity incident	PTPR	Under proposed § 1582.223, covered entities would be required to implement into its COIP capabilities to respond to cybersecurity incidents affecting Critical Cyber Systems that audit unauthorized access to internet domains and addresses and document and audit any communications between the OT system and an internal or external system that deviates from the covered entities identified baseline of communication; identify and respond to execution of unauthorized code, including macro scripts; and define, prioritize, and drive standardized incident response activities, such as Security, Orchestration, Automation, and Response (SOAR).	Partially for railroad carriers. 6 USC 1162(e)(1)(C) stipulates the Secretary require that each security plan of a railroad carrier assigned to a high-risk tier includes procedures to be implemented or used by the railroad carrier in response to a terrorist attack. 6 USC 1162(e)(1)(G) stipulates the Secretary require that each security plan of a railroad carrier assigned to a high-risk tier includes plans for providing redundant and backup systems required to ensure the continued operation of critical elements of the railroad carrier's system in the event of a terrorist attack or other incident. Partially for public transportation. 6 USC 1134(c)(1)(A) stipulates that the Secretary require public transportation agencies determined by the Secretary to be high risk to develop a comprehensive security plan; 6 USC 1134(c)(2)(F) and (H) require that the Secretary ensure that security plans for high-risk public transportation agencies include plans for providing redundant and other appropriate	Cost captured in Reporting and Detection of Cyber Incidents

49 CFR Part	Affected Industry	Requirements/Burden	Specifically Required by Statute?[363]	Ten-Year Cost to Industry or TSA ($ Thousands)
			backup systems necessary to ensure the continued operation of critical elements of the public transportation system in the event of a terrorist attack or other major incident and methods to mitigate damage within a public transportation system in case of an attack on the system, including a plan for communication and coordination with emergency responders.	
§ 1582.225 Reporting cybersecurity incidents	PTPR	Under proposed § 1582.225, covered entities would be required to implement incident response plans that include reporting within 24 hours to CISA and include the reporting person's name, phone number, and email progress, the location of the incident with identifying information, a description of the incident, and any additional relevant information.	No	**PTPR: $9.7**
§ 1582.227 Cybersecurity Incident Response Plan	PTPR	Under proposed § 1582.227, covered entities would be required to have a plan to ensure the impacts of incidents are limited, data backups are tested before use, isolation measures are put into place to reduce risks, and identification of who is responsible for implementing the plan.	Partially for railroad carriers. 6 USC 1162(e)(1)(C) stipulates that the Secretary require each security plan of a railroad carrier assigned to a high-risk tier includes procedures to be implemented or used by the railroad carrier in response to a terrorist attack. 6 USC 1162(e)(1)(G) stipulates that the Secretary require each security plan of a railroad carrier assigned to a high-risk tier includes plans for providing redundant and backup systems required to ensure the continued operation of critical elements of the railroad carrier's system in the event of a terrorist attack or other incident.	PTPR: $5,257.7 TSA: $64.0 Total: $5,321.6

49 CFR Part	Affected Industry	Requirements/Burden	Specifically Required by Statute?[363]	Ten-Year Cost to Industry or TSA ($ Thousands)
			Partially for public transportation. 6 USC 1134(c)(2)(F) requires that the Secretary ensure each high-risk public transportation agency security plan includes plans for providing redundant and other appropriate backup systems necessary to ensure the continued operation of critical elements of the public transportation system in the event of a terrorist attack or other major incident. 6 USC 1134(c)(2)(G) requires that the Secretary ensure each high-risk public transportation agency security plan includes plans for providing service capabilities throughout the system in the event of a terrorist attack or other major incident in the city or region where the public transportation system serves. 6 USC 1134(c)(2)(H) requires that the Secretary ensure each high-risk public transportation agency security plan includes methods to mitigate damage within a public transportation system in case of an attack on the system, including a plan for communication and coordination with emergency responders.	
§ 1582.229 Cybersecurity Assessment Plan	PTPR	Under proposed § 1582.229, covered entities would be required to have a CAP that allowed owner/operators to conduct their own bi-annual cybersecurity design review. The CAP must include a	No	PTPR: $5,794.9 TSA: $671.7 **Total: $6,466.6**

49 CFR Part	Affected Industry	Requirements/Burden	Specifically Required by Statute?[363]	Ten-Year Cost to Industry or TSA ($ Thousands)
		specific schedule for assessments to ensure that at least 30 percent of the COIP is tested each year at a pace to ensure 100 percent is assessed over any 3-year period.		
§ 1582.231 Documentation to establish compliance	PTPR	Under proposed § 1582.231, covered entities would be required to, at the request of TSA, provide evidence of compliance, including copies of records if requested, sufficient to demonstrate compliance.	No	**PTPR: $645.7**
1584 - Highway and Motor Carrier Security				
§ 1584.101 Scope	OTRB	Provision 101 adds a scope to Part 1584 for the proposed rule and clarifying which entities would be covered by the applicability of the proposed rule based on TSA's exercise of its discretion. Includes costs associated with determining applicability and entity familiarization with the rule.	No	**OTRB: $206.2**
§ 1584.107 Reporting cybersecurity incidents	OTRB	Under proposed § 1584.107, covered entities would be required to implement incident response plans that include reporting within 24 hours to CISA and include the reporting person's name, phone number, and email progress, the location of the incident with identifying information, a description of the incident, and any additional relevant information.	Partially. 6 USC 1181(e)(1)(H) stipulates that the Secretary require each security plan of an over-the-road bus operator assigned to a high-risk tier includes such other actions or procedures as the Secretary determines are appropriate to address the security of over-the-road bus operators.	**OTRB: $9.8**
1586 - Pipeline Facilities and Systems Security				
§ 1586.101 Scope	Pipeline	Provision 101 adds a scope to Part 1586 for the proposed rule.	No	Not Quantified/Procedural
§ 1586.103 Physical Security Coordinator	Pipeline	Adding proposed § 1586.103, which describes the requirement to designate a primary and at least one alternate Physical Security Coordinator and the types of biographic information that must be provided to TSA.	No	**Pipeline: $31.9**
§ 1586.105 Reporting of significant physical security concerns	Pipeline	Adding proposed § 1586.105, which describes the requirement to report physical security incidents to TSA and details the information that must be provided.	No	Pipeline: $133.0 TSA: $526.5 **Total: $659.5**
§ 1586.201 Scope and applicability	Pipeline	Adding a scope to proposed part 1582 subpart D and clarifying which entities would be covered by the applicability of the proposed rule based on TSA's exercise of its discretion. Includes costs	No	**Pipeline: $852.0**

49 CFR Part	Affected Industry	Requirements/Burden	Specifically Required by Statute?[363]	Ten-Year Cost to Industry or TSA ($ Thousands)
		associated with determining applicability and entity familiarization with the rule.		
§ 1586.203 Form, content, and availability of Cybersecurity Risk Management program	Pipeline	Adding proposed § 1586.203, which describes the form that a CRM program should take in addition to its content and the availability to access said program information.	No	Not Quantified/Procedural. Costs for CRM Program elements are captured in individual CFR Sections.
§ 1586.205 Cybersecurity evaluation	Pipeline	Under proposed § 1586.205 covered entities must assess their cybersecurity systems annually and notify TSA within seven days of completing said assessments in addition to making said assessments available to TSA.	No	Pipeline: $6,834.9 TSA: $260.2 **Total: $7,095.1**
§ 1586.207 Cybersecurity Operational Implementation Plan	Pipeline	Under proposed § 1586.207, covered entities would be required to include their defense plans, physical and logical/virtual security controls, and compliance with other sections of this rule within their COIPs.	No	Specific cost elements of the COIP are included under §1586.209, §1586.211, §1586.213, §1586.215, and §1586.217.
§ 1586.209 Governance of the CRM program	Pipeline	Under proposed § 1586.209, covered entities would be required to identify and designate an accountable executive for the CRM program. This individual's contact and identifying information must be provided to TSA and incorporated into the COIP. The cost of this provision also includes time to create and maintain the COIP.	No	Pipeline: $3,167.4 TSA: $3,333.7 **Total: $6,501.1**
§ 1586.211 Cybersecurity Coordinator	Pipeline	Under proposed § 1586.211, covered entities would be required to identify and designate a primary and at least one alternate Cybersecurity coordinator who is accessible to TSA 24 hours a day seven days a week. The name, title, phone numbers, and email addresses of the coordinators and their alternatives must be given to TSA.	No	Pipeline: $161.9 TSA: $32.7 **Total: $194.6**
§ 1586.213 Identification of Critical Cyber Systems	Pipeline	Under proposed § 1586.213, covered entities would be required to identify critical cyber systems, including both OT and IT systems. These systems will need to be incorporated into the COIP and include specific identifying information for the system in addition to the manufacturer or designer for each system.	No	**Pipeline: $4,185.6**
§ 1586.215 Supply chain risk management	Pipeline	Under proposed § 1586.215, covered entities would be required to incorporate supply chain incident reporting into their procurement documents and contracts, ensure that these documents stipulate	No	**Pipeline: $26,321.3**

49 CFR Part	Affected Industry	Requirements/Burden	Specifically Required by Statute?[363]	Ten-Year Cost to Industry or TSA ($ Thousands)
		vendors or service providers notify the procuring customer of security vulnerabilities within a risk-informed time frame, and that the documents include cybersecurity requirements and questions.		
§ 1586.217 Protection of Critical Cyber Systems	Pipeline	Under proposed § 1586.217, covered entities would be required to describe their network segmentation policies and controls necessary to address cybersecurity threats. This includes implementing network segmentation of critical systems, managing identification and authentication policies, implementing multi-factor authentication, implementing zero trust policies, ensuring that all critical cyber systems are up to date on patches, storing logging data in a secured and centralized system, and ensure that backups are stored in a secure manner and are free of malicious code.	No	**Pipeline: $437,172.2**
§ 1586.219 Cybersecurity training and knowledge	Pipeline	Under proposed § 1586.219, covered entities would be required to provide a baseline of cybersecurity training to all employees with access to the entity's IT or OT system annually and additional training to employees with roles and responsibilities for implementing the CRM program.	No	Pipeline: $27,016.5 TSA: $554.9 **Total: $27,571.4**
§ 1586.221 Detection of cybersecurity incidents	Pipeline	Under proposed § 1586.221, covered entities would be required to ensure continuous monitoring and detection policies that identify cybersecurity incidents as they occur and automatic measures in place to mitigate the impact.	No	**Pipeline: $7,739.9**
§ 1586.223 Capabilities to respond to a cybersecurity incident	Pipeline	Under proposed § 1582.223, covered entities would be required to implement into its COIP capabilities to respond to cybersecurity incidents affecting Critical Cyber Systems that audit unauthorized access to internet domains and addresses and document and audit any communications between the OT system and an internal or external system that deviates from the covered entities identified baseline of communication; identify and respond to execution of unauthorized code, including macro scripts; and define, prioritize, and drive standardized incident response activities, such as Security, Orchestration, Automation, and Response (SOAR).	No	Cost captured in Reporting and Detection of Cyber Incidents
§ 1586.225 Reporting cybersecurity incidents	Pipeline	Under proposed § 1586.225, covered entities would be required to implement incident response plans that include reporting within 24 hours to CISA and include the reporting person's name, phone number, and email progress, the location of the incident with identifying information, a description of the incident, and any additional relevant information.	No	**Pipeline: $265.8**

49 CFR Part	Affected Industry	Requirements/Burden	Specifically Required by Statute?[363]	Ten-Year Cost to Industry or TSA ($ Thousands)
§ 1586.227 Cybersecurity Incident Response Plan	Pipeline	Under proposed § 1586.227, covered entities would be required to have a plan to ensure the impacts of incidents are limited, data backups are tested before use, isolation measures are put into place to reduce risks, and identification of who is responsible for implementing the plan.	No	Pipeline: $43,406.3 TSA: $1,361.3 **Total: $44,767.5**
§ 1586.229 Cybersecurity Assessment Plan	Pipeline	Under proposed § 1586.229, covered entities would be required to have a CAP that allowed owner/operators to conduct their own bi-annual cybersecurity design review. The CAP must include a specific schedule for assessments to ensure that at least 30 percent of the COIP is tested each year at a pace to ensure 100 percent is assessed over any 3-year period.	No	Pipeline: $18,367.2 TSA: $2,081.7 **Total: $20,448.9**
§ 1586.231 Documentation to establish compliance	Pipeline	Under proposed § 1586.231, covered entities would be required to, at the request of TSA, provide evidence of compliance, including copies of records if requested, sufficient to demonstrate compliance.	No	**Pipeline: $4,527.4**

3.7 Security Directive Comparison

Since 2021, TSA has issued SDs (with renewals and revisions) to higher-risk freight railroads, passenger rail owner/operators, and pipeline owner/operators as shown in Table 3-97. The proposed rule includes many of the same requirements found in TSA's SDs. The cost analysis presented throughout the preceding sections, however, does not assume that the requirements in the SDs are being implemented and captures the full cost of the CRM program. Similarly, TSA has not attempted to provide a baseline that assumes industry implementation of cybersecurity best practices. While TSA recognizes that many owner/operators have already incurred costs to implement a variety of cybersecurity protection and risk management measures, the time and resources expended to implement these measures are unknown and have been incurred independent of this proposed regulation. At the same time, this rulemaking does not pivot away in a new direction different from what is required by the SDs in recognition of the investments made by the industry in enhancing their cybersecurity posture as required by the SDs and in anticipation of TSA codifying those requirements through this rulemaking. This section provides cost estimates for "new" requirements under the rule as compared to SD cost estimates which helps illustrate the incremental increase of the rule relative to the SDs. TSA requests comment on the assumptions and estimates presented within this section.

Table 3-97: TSA's SDs and ICs by Date and Number of Entities Affected

Industry Notice	Effective Date	Freight Railroad	PTPR	OTRB	Pipeline
SD Pipeline-2021-01	May 28, 2021	0	0	0	100
SD Pipeline-2021-02	July 26, 2021	0	0	0	100
SD Pipeline-2021-01A	December 1, 2021	0	0	0	96
SD Pipeline-2021-02B	December 17, 2021	0	0	0	96
SD 1580-21-01	December 31, 2021	62	0	0	0
SD 1582-21-01	December 31, 2021	0	31	0	0
ST IC-2021-01	December 31, 2021	395	84	71	0
IC Pipeline-2022-01	February 16, 2022	0	0	0	2900
ST IC-2022-01	February 25, 2022	395	84	71	0
ST IC-2022-02	March 23, 2022	395	84	71	2900

Industry Notice	Effective Date	Freight Railroad	PTPR	OTRB	Pipeline
SD Pipeline-2021-01B	May 29, 2022	0	0	0	96
SD Pipeline-2021-02C	July 27, 2022	0	0	0	96
SD 1580-21-01A	October 24, 2022	62	0	0	0
SD 1582-21-01A	October 24, 2022	0	31	0	0
SD 1580/82-2022-01	October 24, 2022	62	5	0	0
SD Pipeline-2021-01C	May 29, 2023	0	0	0	91
SD Pipeline-2021-02D	July 27, 2023	0	0	0	91
NPRM	TBD	73	34	71	115

Section 1.7.1 identifies the key elements of the rulemaking that are not previously included in TSA SDs including any changes to the SDs. These new requirements include: (1) cybersecurity training for Freight Rail, PTPR, and Pipeline owner/operators, (2) supply chain risk management within the COIP for Freight Rail, PTPR, and Pipeline owner/operators, (3) designation of an accountable executive for Freight Rail, PTPR, and Pipeline owner/operators, (4) identification of the baseline of acceptable communications between IT and OT systems; (5) requirements for the owner/operator to identify any operational needs that prevent or delay implementation of the CRM program requirements for critical systems; (6) a completion date for the POAM within three years; and (7) cybersecurity incident reporting to CISA for OTRB owner/operators.

These new requirements result in additional costs to industry relative to any current efforts to comply with SDs. TSA separates these cost elements from the primary analysis to show the incremental increase in costs for the rulemaking versus the SDs. However, a number of cost items do not have a specific hour burden tied to them as they are highly variable between owner/operators and thus not estimated below. For example, baseline of acceptable communications between IT and OT systems (which is part of the COIP), identification of operational needs that might prevent or delay implementation, and the POAM completion date. Table 3-98 presents the costs of requirements previously included under the SDs for Freight Rail, PTPR, and Pipeline entities subject to the previously issued SDs, as well as costs incurred by

TSA.[364]

Table 3-98: SD Requirement Costs ($ Thousands)

Year	SD Requirement Costs for Freight Rail	SD Requirement Costs for PTPR	SD Requirement Costs for Pipeline	SD Requirement Costs for TSA	Total SD Requirement Costs d = ∑a,b,c,d		
	a	b	c	d	Undiscounted	Discounted at 3%	Discounted at 7%
1	$72,005.0	$93,717.0	$64,373.1	$2,982.5	$233,077.5	$226,288.9	$217,829.47
2	$70,750.91	$94,380.71	$61,549.28	$1,996.87	$228,677.76	$215,550.72	$199,736.01
3	$69,979.37	$94,994.87	$59,869.05	$2,000.34	$226,843.62	$207,594.05	$185,171.97
4	$71,949.92	$96,975.58	$62,438.34	$1,102.69	$232,466.53	$206,543.50	$177,347.60
5	$71,205.94	$97,636.95	$60,776.96	$1,106.31	$230,726.14	$199,026.40	$164,504.55
6	$73,267.24	$99,703.89	$63,465.46	$1,109.89	$237,546.48	$198,941.44	$158,287.25
7	$72,544.79	$100,415.10	$61,823.58	$1,113.55	$235,897.03	$191,805.87	$146,904.81
8	$74,632.70	$102,537.74	$64,532.23	$1,117.31	$242,819.97	$191,684.33	$141,323.43
9	$73,937.18	$103,301.48	$62,910.82	$1,121.05	$241,270.54	$184,913.78	$131,235.19
10	$76,052.51	$105,482.11	$65,640.26	$1,124.95	$248,299.82	$184,758.39	$126,223.04
Total	**$726,325.5**	**$989,145.4**	**$627,379.0**	**$14,775.5**	**$2,357,625.4**	**$2,007,107.3**	**$1,648,563.3**

Note: Totals may not add due to rounding. The costs in this table include only the costs of SD requirements on currently covered entities, not new entities who would now be subject under this rulemaking.

Table 3-99 displays the new requirements cost as well as an estimated cost of the SD requirements for the freight rail industry. This includes an estimate of the SD related costs for 11 freight rail entities (or approximately 15.07 percent of all freight rail entities) that are newly covered under this rule but were not previously covered under the SDs. TSA estimates the cost of the new requirements plus the cost to newly covered entities to total $253.4 million undiscounted over 10 years which makes up 26 percent of the overall estimated cost to the freight rail industry.

[364] This includes all costs except for those associated with designating an accountable executive, supply chain risk management, and cybersecurity training costs as well as OTRB cybersecurity incident reporting. It also does not include newly covered entities under the rule.

Table 3-99: SD Cost Comparison for Freight Rail ($ Thousands)

Year	New Requirement Costs				Total New Requirement Costs	SD Requirement Costs (including familiarization, documentation)	Total Costs for Freight Rail
	Accountable Executive	Supply Chain Risk Management	Training	New Entity Cost			
	a = Column e, Table 3-4	b = Table 3-7	c = Table 3-13 + Table 3-14	d = (Column h, Table 3-25 – ∑a,b,c) x 15.07%	e = a + b + c + d	f = Column a, Table 3-98	g = e + f
1	$28.3	$2,356.7	$10,485.5	$12,776.6	$25,647.1	$72,005.0	$97,652.0
2	$1.4	$2,375.1	$9,789.9	$12,554.1	$24,720.5	$70,750.9	$95,471.4
3	$1.4	$2,393.5	$9,831.0	$12,417.2	$24,643.1	$69,979.4	$94,622.4
4	$1.4	$2,412.3	$9,872.4	$12,766.8	$25,052.8	$71,949.9	$97,002.7
5	$1.4	$2,431.3	$9,913.9	$12,634.8	$24,981.4	$71,205.9	$96,187.3
6	$1.4	$2,450.3	$9,955.5	$13,000.6	$25,407.8	$73,267.2	$98,675.1
7	$1.4	$2,469.4	$9,997.3	$12,872.4	$25,340.5	$72,544.8	$97,885.3
8	$1.4	$2,488.8	$10,039.4	$13,242.8	$25,772.4	$74,632.7	$100,405.1
9	$1.4	$2,508.1	$10,081.5	$13,119.4	$25,710.5	$73,937.2	$99,647.7
10	$1.4	$2,527.8	$10,123.9	$13,494.8	$26,148.0	$76,052.5	$102,200.5
Total	**$40.9**	**$24,413.4**	**$100,090.4**	**$128,879.4**	**$253,424.1**	**$726,325.5**	**$979,749.6**

Note: Totals may not add due to rounding.

Table 3-100 displays the new requirements cost as well as an estimated cost of the SD requirements for the PTPR industry. This includes an estimate of the SD related costs for 3 PTPR entities (or approximately 8.82 percent of all PTPR entities) that are newly covered under this rule but were not previously covered under the SDs. TSA estimates the cost of the new requirements plus the cost to newly covered entities to total $274.4 million undiscounted over 10 years which makes up 22 percent of the overall estimated cost to the PTPR industry.

Table 3-100: SD Cost Comparison for PTPR ($ Thousands)

Year	New Requirement Costs				Total New Requirement Costs	SD Requirement Costs (including familiarization, documentation)	Total Costs for PTPR
	Accountable Executive	Supply Chain Risk Management	Training	New Entity Cost			
	a = Column e, Table 3-29	b = Table 3-32	c = Table 3-38 + Table 3-39	d = (Column h, Table 3-50 - ∑a,b,c) x 8.82%	e = a + b + c + d	f = Column b, Table 3-98	g = e + f
1	$8.5	$944.7	$16,260.7	$9,065.4	$26,279.3	$93,717.0	$119,996.3
2	$1.3	$965.3	$16,156.4	$9,129.6	$26,252.6	$94,380.7	$120,633.3
3	$1.3	$986.7	$16,335.9	$9,189.0	$26,513.0	$94,994.9	$121,507.8
4	$1.4	$1,008.1	$16,517.2	$9,380.6	$26,907.2	$96,975.6	$123,882.8
5	$1.4	$1,030.3	$16,700.7	$9,444.6	$27,177.0	$97,636.9	$124,813.9
6	$1.4	$1,052.8	$16,886.1	$9,644.5	$27,584.9	$99,703.9	$127,288.7
7	$1.5	$1,075.9	$17,073.6	$9,713.3	$27,864.3	$100,415.1	$128,279.4
8	$1.5	$1,099.5	$17,263.2	$9,918.7	$28,282.9	$102,537.7	$130,820.6
9	$1.5	$1,123.4	$17,454.8	$9,992.5	$28,572.3	$103,301.5	$131,873.8
10	$1.6	$1,148.1	$17,648.8	$10,203.5	$29,001.9	$105,482.1	$134,484.0
Total	**$21.5**	**$10,434.8**	**$168,297.3**	**$95,681.8**	**$274,435.3**	**$989,145.4**	**$1,263,580.7**

Note: Totals may not add due to rounding.

Table 3-101 displays the new requirements cost as well as an estimated cost of the SD requirements for the pipeline industry. This includes an estimate of the SD related costs for 19 pipeline entities (or approximately 16.52 percent of all PTPR entities) that are newly covered under this rule but were not previously covered under the SDs. TSA estimates the cost of the new requirements plus the cost to newly covered entities to total $200.0 million undiscounted over 10 years which makes up 24 percent of the overall estimated cost to the pipeline industry.

Table 3-101: SD Cost Comparison for Pipeline ($ Thousands)

Year	New Requirement Costs				Total New Requirement Costs	SD Requirement Costs (including familiarization, documentation)	Total Costs for Pipeline
	Accountable Executive	Supply Chain Risk Management	Training	New Entity Cost			
	a = Column e, Table 3-59	b = Table 3-62	c = Table 3-68 + Table 3-69	d = (Column i, Table 3-80 - ∑a,b,c) x 16.52%	e = a + b + c + d	f = Column c, Table 3-98	g = e + f
1	$78.0	$3,747.6	$4,698.6	$12,738.9	$21,263.1	$64,373.1	$85,636.2
2	$10.7	$3,747.6	$3,634.6	$12,180.1	$19,572.9	$61,549.3	$81,122.2
3	$10.7	$3,747.6	$3,657.2	$11,847.6	$19,263.0	$59,869.1	$79,132.0
4	$10.7	$3,747.6	$3,679.8	$12,356.0	$19,794.1	$62,438.3	$82,232.4
5	$10.7	$3,747.6	$3,702.6	$12,027.3	$19,488.1	$60,777.0	$80,265.1
6	$10.7	$3,747.6	$3,725.6	$12,559.3	$20,043.1	$63,465.5	$83,508.6
7	$10.7	$3,747.6	$3,748.7	$12,234.4	$19,741.3	$61,823.6	$81,564.9
8	$10.7	$3,747.6	$3,771.9	$12,770.4	$20,300.6	$64,532.2	$84,832.8
9	$10.7	$3,747.6	$3,795.3	$12,449.5	$20,003.1	$62,910.8	$82,913.9
10	$10.7	$3,747.6	$3,818.9	$12,989.7	$20,566.7	$65,640.3	$86,207.0
Total	**$174.0**	**$37,475.6**	**$38,233.3**	**$124,153.1**	**$200,036.0**	**$627,379.0**	**$827,415.1**

Note: Totals may not add due to rounding.

Table 3-102 displays the new requirements cost as well as an estimated cost of the SD requirements for TSA. This includes an estimate of the SD related costs for 33 new entities across the three industries (or approximately 14.86 percent of all entities) that are newly covered under this rule but were not previously covered under the SDs. TSA estimates the cost of the new requirements plus cost resulting from newly covered entities to total $4.1 million undiscounted over 10 years which makes up 22 percent of the overall estimated cost to TSA.

Table 3-102: SD Cost Comparison for TSA ($ Thousands)

Year	New Requirement Costs			Total New Requirement Costs	SD Requirement Costs (including familiarization, documentation)	Total Costs for TSA
	Accountable Executive	Training	New Entity Cost			
	a = Table 3-85	b = Table 3-87 + Table 3-88	c = (Column f, Table 3-92 - ∑a,b) x 14.86%	d = a + b + c	e = Column d, Table 3-98	f = d + e
1	$89.4	$834.0	$520.6	$1,443.9	$2,982.5	$4,426.4
2	$9.9	$52.4	$348.5	$410.8	$1,996.9	$2,407.7
3	$9.9	$52.8	$349.1	$411.9	$2,000.3	$2,412.2
4	$10.0	$53.1	$192.5	$255.6	$1,102.7	$1,358.2
5	$10.0	$53.6	$193.1	$256.7	$1,106.3	$1,363.0
6	$10.1	$53.9	$193.7	$257.7	$1,109.9	$1,367.6
7	$10.2	$54.3	$194.4	$258.8	$1,113.6	$1,372.3
8	$10.2	$54.7	$195.0	$259.9	$1,117.3	$1,377.2
9	$10.3	$55.0	$195.7	$261.0	$1,121.1	$1,382.0
10	$10.4	$55.5	$196.3	$262.2	$1,125.0	$1,387.1
Total	**$180.3**	**$1,319.2**	**$2,578.8**	**$4,078.4**	**$14,775.5**	**$18,853.8**

Note: Totals may not add due to rounding.

Table 3-103 displays the total costs of new requirements across all industries and TSA compared to the total cost of requirements included under the SDs. This table also includes costs to OTRB entities, as the requirements applicable to OTRB under this rule were not previously covered by a SD. TSA estimates the cost of the new requirements and cost resulting from new entities across all industries and TSA to total $732.2 million undiscounted over 10 years which makes up 24 percent of the overall estimated cost of the rule.

Table 3-103: Total SD Cost Comparison ($ Thousands)

Year	New Requirement Costs					Total New Requirement Costs	SD Requirement Costs (including familiarization, documentation)	Total Costs
	Account-able Executive	Supply Chain Risk Manage-ment	Training	New Entity Cost	OTRB Costs			
	a	b	c	d	e	f = a + b + c + d + e	g	h = f + g
1	$204.3	$7,049.0	$32,278.8	$35,101.4	$188.5	$74,822.0	$233,077.5	$307,899.5
2	$23.2	$7,088.0	$29,633.3	$34,212.3	$6.0	$70,962.8	$228,677.8	$299,640.5
3	$23.3	$7,127.8	$29,876.9	$33,802.9	$6.1	$70,837.0	$226,843.6	$297,680.6
4	$23.4	$7,167.9	$30,122.5	$34,695.9	$6.3	$72,016.0	$232,466.5	$304,482.5
5	$23.5	$7,209.2	$30,370.8	$34,299.7	$6.4	$71,909.7	$230,726.1	$302,635.8
6	$23.6	$7,250.7	$30,621.1	$35,398.1	$6.6	$73,300.1	$237,546.5	$310,846.6
7	$23.7	$7,292.8	$30,873.9	$35,014.4	$6.8	$73,211.6	$235,897.0	$309,108.6
8	$23.8	$7,335.8	$31,129.2	$36,126.9	$6.9	$74,622.7	$242,820.0	$317,442.6
9	$23.9	$7,379.1	$31,386.7	$35,757.2	$7.1	$74,554.0	$241,270.5	$315,824.5
10	$24.0	$7,423.5	$31,647.0	$36,884.3	$7.3	$75,986.1	$248,299.8	$324,285.9
Total	**$416.8**	**$72,323.8**	**$307,940.2**	**$351,293.1**	**$247.9**	**$732,221.8**	**$2,357,625.4**	**$3,089,847.2**

Note: Totals may not add due to rounding.

3.8 Sensitivity Analysis

Cybersecurity is constantly evolving and there is a range of means to implement cybersecurity measures as well as a spectrum of maturity across the transportation industry. The primary cost analysis presents costs using industry average estimates which is in part based on what TSA expects owner/operators would do to satisfy the rule's requirements. The primary analysis also uses a zero-baseline assumption which presumes regulated industries have not implemented any measures that would meet the rule's requirements; thereby capturing the full cost of the requirement as if they were completely new. There is inherent uncertainty with such cost estimates as well as the degree to which industry actions may already satisfy the rule's requirements. This section presents a sensitivity analysis that assesses both potential less expensive measures that would satisfy the regulations and to what extent these measures, or other actions, may already be implemented across the industry and thus reduce the estimated cost of the rule. 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.

Most of the costs detailed previously in Section 3 are a result of three primary cost drivers: access control implementation, Critical Cyber System data backups, and cybersecurity training. TSA assesses each of these cost drivers based on how owner/operators of various sizes and complexity in operations may comply with the requirements. This assessment considers the actions or activities such owner/operators would take, as well as the extent to which they may already be taking action consistent with the proposed requirements. However, please note that the differing measures and proportions of industry employing each measure are largely based on SME insight and do not reflect an in-depth investigation of current practices or compliance with SDs, but do include support references where available.

Nonetheless, this sensitivity analysis identifies specific uncertainties for the three main cost drivers and discusses both quantitatively and qualitatively how the total practical impacts of the proposed rule may vary as a result.

3.8.1 Access Control

Sections 1580.317(b)(2), 1582.217(b)(2), and 1586.217(b)(2) of the NPRM detail specific access control measures for Critical Cyber Systems that must be incorporated, including multi-factor authentication (MFA) or other logical/virtual and physical security controls to provide risk mitigation commensurate to MFA. Earlier in Section 3 of this analysis, TSA assumes all entities would satisfy this access control requirement by requiring use of MFA for all employees. MFA requires users to engage with at least two factors, such as a personal password or pin plus text message confirmation or access card, before gaining access to a system. TSA assumes implementation of MFA is enabled by the use of a third-party authenticator app that must be

purchased for everyone requiring access to the system. While MFA is thought to be a secure method for complying with this requirement, it is also costly due to the purchase of additional software and the additional time spent for each employee to access daily.

While TSA assumes all entities would use MFA to satisfy this requirement in the cost analysis, there is likely variability in the actions each owner/operator would take to comply with the access control requirement. There are alternate measures entities may take to restrict both IT and OT access. Most entities already use some form of authentication to restrict IT or OT system access, such as a combination of single factor authentication and physical security restrictions, which may be sufficient to capture the level of access control needed to comply with the requirement. To control OT access, entities may be able to restrict physical access, even with a multi-factor process, to control rooms where their OT systems are contained, eliminating the need for MFA for all employees. Other examples of alternate methods to comply with this requirement may include, but are not exclusive to, more extensive and expansive access measures that could include biometric identification via fingerprint or requiring a second individual be present with a combined combination of passwords needed to access restricted areas or as minimal as removing critical systems from a shared network space. If the owner/operator chooses to use methods of access control other than MFA, the proposed rule would require those methods to provide mitigation commensurate with MFA. The variability in these methods also introduces variability in the cost each entity would incur, with alternate methods likely to be less costly than the MFA option previously presented in Section 3.

In addition to uncertainty regarding the actions that will be taken to satisfy this requirement, there is also uncertainty surrounding existing industry efforts. Many entities may already be

engaged in some form of single factor or MFA to varying degrees.[365] For example, an owner/operator may use MFA in some locations but not others, or for a subset of their employees but not all. Other entities may already use MFA for all employees and would therefore incur no additional costs as a result of this rule. Therefore, the practical costs to satisfy this requirement may be less than the costs for access control presented previously in Section 3. Given this uncertainty, TSA analyzes the impact on the total cost of the rule assuming 25 percent of entities have already implemented MFA for access control to an extent that would satisfy this requirement; 25 percent would require an incremental increase of their existing partially compliant access control in order to reach compliance; and 50 percent of entities would incur the full per-entity cost calculated in Section 3 or experience cost reductions similar to those resulting from such assumptions. The access control implementation cost alterations are summarized in Table 3-104.

[365] See, *e.g.*, National Institute of Standards and Technology. "Out with the old, in with the new: making MFA the norm." NIST, December 2019. https://www.nist.gov/blogs/cybersecurity-insights/out-old-new-making-mfa-norm, and Deighton, Katie. "Tech Companies Push Users to Adopt Two-Factor Authentication." The Wall Street Journal, November 2021. https://www.wsj.com/articles/tech-companies-push-users-to-adopt-two-factor-authentication-11635807088.

Table 3-104: Primary vs. Sensitivity Analysis: Access Control Assumptions

Level of Compliance with Access Control Requirement	Primary Analysis		Sensitivity Analysis	
	Assumed Percentage of Affected Entities	Measures Necessary to Reach Compliance	Assumed Percentage of Affected Entities	Measures Necessary to Reach Compliance
Full compliance	0%	-	25%	None
Partial compliance	0%	-	25%	Entities scale from the use of single-factor authentication to multi-factor authentication. TSA assumes a 50% reduction in cost with results in a software cost of $36 per employee and a use time of 3.59 hours per employee.
No compliance (Zero –Baseline)	100%	Purchase of MFA software at a cost of $72 per employee and a use time of 7.17 hours per employee.	50%	Entities engage in full implementation of MFA as discussed in Section 3. This results in a software cost of $72 per employee and a use time of 7.17 hours per employee.

Based on the above sensitivity assumptions, TSA calculates an alternate total cost per industry for access control implementation. The overall costs of access control implementation, updated with the sensitivity analysis assumptions, are shown for each mode in Table 3-105, Table 3-106, and Table 3-107. For comparison purposes, the primary analysis access control-specific costs per industry are also presented in each table.

Table 3-105: Sensitivity Access Control Costs, Freight Rail ($ Thousands)

Year	Employee Population Plus Growth	MFA Equipment Cost	MFA Implementation Cost	Total Sensitivity Access Control Cost	Total Primary Access Control Cost
	a = Column a, Table 2-2	b = a × (25% × $0 + 25% × $36 + 50%) × $72)	c = a × (25% × 0 hours + 25% × 3.59 hours + 50% × 7.17 hours) × $53.19	d = b + c	e = Table 3-10
1	116,960.00	$5,263.2	$27,886.1	$33,149.3	$53,026.4
2	117,451.23	$5,285.3	$28,003.2	$33,288.5	$53,249.1
3	117,944.53	$5,307.5	$28,120.8	$33,428.3	$53,472.8
4	118,439.89	$5,329.8	$28,238.9	$33,568.7	$53,697.4
5	118,937.34	$5,352.2	$28,357.5	$33,709.7	$53,922.9
6	119,436.88	$5,374.7	$28,476.6	$33,851.3	$54,149.4
7	119,938.51	$5,397.2	$28,596.2	$33,993.5	$54,376.8
8	120,442.26	$5,419.9	$28,716.3	$34,136.2	$54,605.2
9	120,948.11	$5,442.7	$28,837.0	$34,279.6	$54,834.5
10	121,456.09	$5,465.5	$28,958.1	$34,423.6	$55,064.8
Total		**$53,638.0**	**$284,190.8**	**$337,828.8**	**$540,399.3**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed Formulas with X_{yn-1} in year one are equal to the initial value of X_{y1}

Table 3-106: Sensitivity Access Control Costs for Implementation, PTPR ($ Thousands)

Year	Employee Population Plus Growth	MFA Equipment Cost	MFA Implementation Cost	Total Sensitivity Access Control Cost	Total Primary Access Control Cost
	a = Column d, Table 2-2	b = a × (25% × $0 + 25% × $36 + 50%) × $72)	c = a × (25% × 0 hours + 25% × 3.59 hours + 50% × 7.17 hours) × $31.23	d = b + c	e = Table 3-35
1	299,680.00	$13,485.6	$41,951.7	$55,437.3	$88,681.0
2	303,006.45	$13,635.3	$42,417.4	$56,052.7	$89,665.4
3	306,369.82	$13,786.6	$42,888.2	$56,674.9	$90,660.7
4	309,770.52	$13,939.7	$43,364.3	$57,304.0	$91,667.0
5	313,208.98	$14,094.4	$43,845.6	$57,940.1	$92,684.5
6	316,685.60	$14,250.9	$44,332.3	$58,583.2	$93,713.3
7	320,200.81	$14,409.0	$44,824.4	$59,233.5	$94,753.5
8	323,755.04	$14,569.0	$45,322.0	$59,891.0	$95,805.3
9	327,348.72	$14,730.7	$45,825.0	$60,555.7	$96,868.7
10	330,982.29	$14,894.2	$46,333.7	$61,227.9	$97,944.0
Total		**$141,795.4**	**$441,104.8**	**$582,900.2**	**$932,443.5**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed. Formulas with X_{yn-1} in year one are equal to the initial value of X_{y1}

Table 3-107: Sensitivity Access Control Implementation Cost, Pipeline ($ Thousands)

Year	Employee Population Plus Growth	MFA Equipment Cost	MFA Implementation Cost	Total Sensitivity Access Control Cost	Total Primary Access Control Cost
	a = Column g, Table 2-2	b = a × (25% × $0 + 25% × $36 + 50%) × $72)	c = a × (25% × 0 hours + 25% × 3.59 hours + 50% × 7.17 hours) × $69.32	d = b + c	e = Table 3-65
1	39,920.00	$1,796.4	$12,404.2	$14,200.6	$22,715.5
2	40,167.50	$1,807.5	$12,481.1	$14,288.7	$22,856.3
3	40,416.54	$1,818.7	$12,558.5	$14,377.3	$22,998.0
4	40,667.13	$1,830.0	$12,636.4	$14,466.4	$23,140.6
5	40,919.26	$1,841.4	$12,714.7	$14,556.1	$23,284.1
6	41,172.96	$1,852.8	$12,793.5	$14,646.3	$23,428.4
7	41,428.23	$1,864.3	$12,872.9	$14,737.1	$23,573.7
8	41,685.09	$1,875.8	$12,952.7	$14,828.5	$23,719.8
9	41,943.54	$1,887.5	$13,033.0	$14,920.4	$23,866.9
10	42,203.59	$1,899.2	$13,113.8	$15,013.0	$24,014.9
Total		**$18,473.6**	**$127,560.8**	**$146,034.4**	**$233,598.1**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed Formulas with X_{yn-1} in year one are equal to the initial value of X_{y1}

Based on these sensitivity assumptions, the projected access control cost, over 10 years of analysis, to freight rail is $202.6 million less (37 percent reduction in cost); the projected cost to PTPR industry is $349.5 million less (37 percent reduction in cost); and the projected cost to pipeline industry is $87.6 million less (37 percent reduction in cost). In total, the projected costs for access control implementation for all industries would be $639.7 million less than the costs estimated previously in Section 3.

3.8.2 Critical Cyber System Data Backups

Sections 1580.317(e), 1582.217(e), and 1586.217(e) of the NPRM require that entities implement policies to ensure all Critical Cyber Systems are backed-up on a regular basis. In Section 3, TSA made several assumptions and estimates to calculate an average owner/operator cost of data backups including the data volume per entity (500 terabytes), growth rate of that data (2.3 percent), and the cost to backup each terabyte of data. However, individual owner/operator's data backup needs will vary based on their unique circumstances which introduces a level of

uncertainty in the actual average cost of data backups. For instance, owner/operators may have less data storage needs or store backups less frequently.

In addition, there is uncertainty surrounding what, if any, existing data backups measures are currently undertaken by covered entities. TSA cybersecurity SMEs believe that many owner/operators likely already back-up critical system data and some storage practices may satisfy requirements in the proposed rule, thereby representing a lower cost than presented in Section 3. This variability in actions currently being taken by the covered entities further obscures the practical incremental impact of the proposed rule.

To assess this variability in practical impacts, TSA re-calculated data backup costs assuming 20 percent of the industry is already sufficiently backing up their critical systems, 50 percent of covered entities would only need an incremental increase to their current system back up, equivalent to half the costs projected in the primary analysis, and the remaining portion of the population would use the original methodology or experience cost reductions similar to those resulting from such assumptions. However, TSA seeks public comment on these assumptions, including what percentage of industry is likely partly or fully backing up critical systems or any other potential cost or data backup system insight.

The application of these assumptions changes the cost of the critical system backups. Table 3-108 summarizes the new sensitivity assumptions and how they differ from the assumptions in the primary analysis.

Table 3-108: Primary vs. Sensitivity Analysis: Critical Cyber System Data Backup Assumptions

Level of Compliance with Access Control Requirement	Primary Analysis		Sensitivity Analysis	
	Assumed Percentage of Affected Entities	Measures Necessary to Reach Compliance	Assumed Percentage of Affected Entities	Measures Necessary to Reach Compliance
Full compliance	0%	-	20%	None
Partial compliance	0%	-	50%	Incremental increase in practices in the primary analysis. Entities would back up only 250 terabytes of data in Year 1.
Baseline	100%	Entities will back up and store Critical Cyber Systems every 500 terabytes of data in Year 1, with a data growth rate of 2.3%	30%	Full implementation of data backups as discussed in Section 3. This means entities would back up 500 terabytes of data in Year 1, with a data growth rate of 2.3%

The costs to each industry under these sensitivity analysis assumptions, wherein 20 percent of entities are fully compliant; 50 percent require an incremental increase in backup practices; and 30 percent will undergo the full implementation of data backup measures as discussed in Section 3, are presented below in Table 3-109, Table 3-110, and Table 3-111. The costs per industry under the primary analysis are presented in each table for comparison.

Table 3-109: Sensitivity Critical Cyber System Data Backup Cost, Freight Rail ($ Thousands)

Year	Freight Rail Population	Critical System Data Size Per Entity (Terabytes)	Cost of Data Backups	Cost of Data Backup Supervision	Total Sensitivity Data Backup Cost	Total Primary Data Backup Cost
	a = Column a, Table 2-1	b = 500 × (1 + 2.30%)^Y_{n-1}	c = a × b × (20% × 0% + 50% × 50% + 30% × 100%) × $329.16	d = a × 12 hours × $64.63	e = c + d	f = Table 3-13
1	73.00	500.00	$6,607.9	$56.6	$6,664.5	$12,071.0
2	73.57	511.50	$6,812.7	$57.1	$6,869.7	$12,443.7
3	74.14	523.26	$7,023.3	$57.5	$7,080.8	$12,827.1
4	74.72	535.29	$7,241.0	$57.9	$7,298.9	$13,223.3
5	75.31	547.60	$7,466.0	$58.4	$7,524.4	$13,632.9
6	75.90	560.19	$7,697.4	$58.9	$7,756.3	$14,054.2
7	76.49	573.07	$7,935.6	$59.3	$7,995.0	$14,487.8
8	77.09	586.25	$8,181.8	$59.8	$8,241.6	$14,935.8
9	77.69	599.73	$8,435.1	$60.3	$8,495.4	$15,396.8
10	78.30	613.52	$8,696.8	$60.7	$8,757.5	$15,873.1
Total			**$76,097.6**	**$586.5**	**$76,684.1**	**$138,945.7**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed. Formulas with X_{yn-1} in year one are equal to the initial value of X_{y1}.

Table 3-110: Sensitivity Critical Cyber System Data Backup Cost, PTPR ($ Thousands)

Year	PTPR Population	Critical System Data Size Per Entity (Terabytes)	Cost of Data Backups	Cost of Data Backup Supervision	Total Sensitivity Data Backup Cost	Total Primary Data Backup Cost
	a = Column d, Table 2-1	b = 500 × (1 + 2.30%)^Y_{n-1}	c = a × b × (20% × 0% + 50% × 50% + 30% × 100%) × $329.16	d = a × 12 hours × $63.63	e = c + d	f = Table 3-37
1	34.00	500.00	$3,077.6	$26.0	$3,103.6	$5,621.7
2	34.74	511.50	$3,217.0	$26.5	$3,243.5	$5,875.5
3	35.51	523.26	$3,363.9	$27.1	$3,391.0	$6,143.2
4	36.28	535.29	$3,515.8	$27.7	$3,543.5	$6,420.1
5	37.08	547.60	$3,676.0	$28.3	$3,704.3	$6,711.9
6	37.89	560.19	$3,842.6	$28.9	$3,871.6	$7,015.5
7	38.72	573.07	$4,017.1	$29.6	$4,046.7	$7,333.4
8	39.57	586.25	$4,199.7	$30.2	$4,229.9	$7,666.0
9	40.43	599.73	$4,389.6	$30.9	$4,420.5	$8,012.0
10	41.32	613.52	$4,589.4	$31.6	$4,621.0	$8,376.0
Total			**$37,888.8**	**$286.7**	**$38,175.5**	**$69,175.4**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed. Formulas with X_{yn-1} in year one are equal to the initial value of X_{y1}.

Table 3-111: Sensitivity Critical Cyber System Data Backup Cost, Pipeline ($ Thousands)

Year	Pipeline Population	Critical System Data Size Per Entity (Terabytes)	Cost of Data Backups	Cost of Data Backup Supervision	Total Sensitivity Data Backup Cost	Total Primary Data Backup Cost
	a = Column j, Table 2-1	b = 500 × (1 + 2.30%)^Y_{n-1}	c = a × b × (20% × 0% + 50% × 50% + 30% × 100%) × $329.16	d = a × 12 hours × $61.21	e = c + d	f = Table 3-67
1	115.00	500.00	$10,409.7	$84.5	$10,494.2	$19,011.2
2	115.00	511.50	$10,649.1	$84.5	$10,733.6	$19,446.5
3	115.00	523.26	$10,893.9	$84.5	$10,978.4	$19,891.6
4	115.00	535.29	$11,144.4	$84.5	$11,228.9	$20,347.0
5	115.00	547.60	$11,400.7	$84.5	$11,485.2	$20,813.0
6	115.00	560.19	$11,662.8	$84.5	$11,747.3	$21,289.6
7	115.00	573.07	$11,931.0	$84.5	$12,015.4	$21,777.1
8	115.00	586.25	$12,205.4	$84.5	$12,289.8	$22,276.0
9	115.00	599.73	$12,486.0	$84.5	$12,570.5	$22,786.3
10	115.00	613.52	$12,773.1	$84.5	$12,857.6	$23,308.3
Total			**$115,556.0**	**$844.7**	**$116,400.7**	**$210,946.6**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed. Formulas with X_{yn-1} in year one are equal to the initial value of X_{y1}

Based on the changes to the data backup assumptions, the Critical Cyber System data backup costs to freight rail would be $62.3 million less; to PTPR would be $31.0 million less; and to pipeline would be $94.5 million less which represents a 45 percent reduction in cost across each mode. In total, the projected costs for all industries for Critical Cyber System data backups would be $187.8 million less than the costs estimated previously in Section 3.

3.8.3 Cybersecurity Training

Sections 1580.319, 1582.219, and 1586.219 of the NPRM detail the requirement for owner/operators to provide basic cybersecurity training to all employees and role-based cybersecurity training to all employees with access to Critical Cyber Systems. Previously in Section 3, TSA assumes all employees within each industry would spend one hour engaged in basic cybersecurity training, while a specific subset of employees, estimated to be 15 percent of the full employee population, would spend two hours engaged in role-based training. In addition to time spent in each training, the cost of this requirement includes time for owner/operators to

create and submit training plans and time for recordkeeping to document each employee's completion of the training.

However, there may be variability in how each owner/operator approaches training and complies with this requirement. For example, such training may include a test-out option for basic cybersecurity training, where individuals can take a brief test of their familiarity with the information that would be provided in the corresponding training. Users who pass this test could satisfy the requirements of the training, and spend less time attending the full training.

Like other requirements, there is also uncertainty surrounding current industry cybersecurity training practices. While TSA assumes previously in Section 3 that all entities would need to create training plans and newly require the cybersecurity training detailed in the NPRM, it may be that many entities have existing elements of the required training and may only need to expand a portion of their plans to encompass the content of each of the required modules detailed in the proposed rule. Further, some owner/operators may already require training that would fully satisfy the rule, while others may only need to supplement existing training to satisfy the rule requirements. This variability in the additional costs entities would incur would reduce the practical cost impact of the proposed rule.

To assess the variable cost impact of this uncertainty, TSA assumes that 20 percent of covered entities already have existing cybersecurity training sufficient to meet the standards and that 50 percent have an existing program that would require only 20 percent of the total time for both the preparation and participation of the training or experience cost reductions like those resulting from such assumptions. The remaining portion of the population (30 percent) would incur the original costs. TSA requests public comment on the likelihood of these assumptions regarding

training practices in industry. Table 3-112 presents a summary of these sensitivity analysis assumptions.

Table 3-112: Cybersecurity Training Sensitivity Analysis Assumptions

Level of Compliance with Access Control Requirement	Primary Analysis		Sensitivity Analysis	
	Assumed Percentage of Affected Entities or Employees	Measures Necessary to Reach Compliance	Assumed Percentage of Affected Entities or Employees	Measures Necessary to Reach Compliance
Full compliance	0%	-	20%	None
Partial compliance	0%	-	50%	Incremental increase in practices in the primary analysis. Entities would require only 20 percent of the total time for both preparation and participation in the training
Baseline	100%	Entities will engage in the full preparation and participation time as described in Section 3.	30%	Full implementation of training as discussed in Section 3.

The impact of these adjusted assumptions on the industry costs for cybersecurity training are presented below in Table 3-113 and Table 3-114 for freight rail; Table 3-115 and Table 3-116 for PTPR; and Table 3-117 and Table 3-118 for pipeline. The costs prior to these changed assumptions, following the methodology detailed previously in Section 3, are presented in each industry-specific cost table for comparison.

Table 3-113: Sensitivity Training Plans Cost for Freight Rail ($ Thousands)

Year	Freight Rail Training Plan Submissions	Total Sensitivity Training Plan Cost	Total Primary Training Plan Cost
	a = Column b, Table 2-1	b = a × (20% × 0 hours + 50% × 16 hours + 30% × 80 hours) × $127.10	c = Table 3-13
1	73.00	$296.9	$742.3
2	0.57	$2.3	$5.8
3	0.57	$2.3	$5.8
4	0.58	$2.4	$5.9
5	0.59	$2.4	$6.0
6	0.59	$2.4	$6.0
7	0.59	$2.4	$6.0
8	0.60	$2.4	$6.1
9	0.60	$2.4	$6.1
10	0.61	$2.5	$6.2
Total		**$318.5**	**$796.2**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed. Formulas with X_{yn-1} in year one are equal to the initial value of X_{y1}.

Table 3-114: Sensitivity Training Participation Costs for Freight Rail ($ Thousands)

Year	Freight Rail Training Population	General Training Cost	Privileged User Training Cost	Training Recordkeeping Cost	Total Sensitivity Training Cost	Total Primary Training Cost
	a = Column a, Table 2-2	b = a × (20% × 0 hours + 50% × .20 hours + 30% × 1.00 hours) × $53.19	c = a × 15% × (20% × 0 hours + 50% × .40 hours + 30% × 2.00 hours) × $97.28	d = (a + (a × 15%)) × 0.02 hours × $40.42	e = b + c + d	f = Table 3-14
1	116,960.00	$2,488.4	$1,365.3	$108.7	$3,962.5	$9,743.2
2	117,451.23	$2,498.9	$1,371.1	$109.2	$3,979.2	$9,784.1
3	117,944.53	$2,509.4	$1,376.8	$109.6	$3,995.9	$9,825.2
4	118,439.89	$2,519.9	$1,382.6	$110.1	$4,012.7	$9,866.5
5	118,937.34	$2,530.5	$1,388.4	$110.6	$4,029.5	$9,907.9
6	119,436.88	$2,541.1	$1,394.3	$111.0	$4,046.4	$9,949.5
7	119,938.51	$2,551.8	$1,400.1	$111.5	$4,063.4	$9,991.3
8	120,442.26	$2,562.5	$1,406.0	$112.0	$4,080.5	$10,033.3
9	120,948.11	$2,573.3	$1,411.9	$112.4	$4,097.6	$10,075.4
10	121,456.09	$2,584.1	$1,417.8	$112.9	$4,114.8	$10,117.7
Total		**$25,360.0**	**$13,914.4**	**$1,108.1**	**$40,382.5**	**$99,294.2**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed Formulas with X_{yn-1} in year one are equal to the initial value of X_{y1}

Table 3-115: Sensitivity Training Plan Costs for PTPR ($ Thousands)

Year	PTPR Training Plan Submissions a = Column e, Table 2-1	Total Sensitivity Training Plan Cost b = (20% × a × 0 hours × $105.82) + (50% × a × 16. hours × $105.82) + (30% × a × 80. hours × $105.82)	Total Primary Training Plan Cost c = Table 3-38
1	34.00	$115.1	$288.8
2	0.74	$2.5	$6.3
3	0.77	$2.6	$6.5
4	0.77	$2.6	$6.5
5	0.80	$2.7	$6.8
6	0.81	$2.7	$6.9
7	0.83	$2.8	$7.0
8	0.85	$2.9	$7.2
9	0.86	$2.9	$7.3
10	0.89	$3.0	$7.6
Total		**$139.9**	**$349.8**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed. Formulas with X_{yn-1} in year one are equal to the initial value of X_{y1}.

Table 3-116: Sensitivity Training Participation Costs for PTPR ($ Thousands)

Year	PTPR Training Population a = Column d, Table 2-2	General Training Cost b = (20% × a × 0 hours × $31.23) + (50% × a × .20 hours × $31.23) + (30% × a × 1.00 hours × $31.23)	Privileged User Training Cost c = (20% × a 15% × 0 hours × $71.26) + (50% × a 15% × .40 hours × $71.26) + (30% × a 15% × 2.00 hours × $71.26)	Training Recordkeeping Cost d = (a + (a × 15%)) × 0.02 hours × $30.07	Total Sensitivity Training Cost e = b + c + d	Total Primary Training Cost f = Table 3-39
1	299,680.00	$3,743.6	$2,562.6	$207.3	$6,513.5	$15,972.8
2	303,006.45	$3,785.2	$2,591.1	$209.6	$6,585.8	$16,150.1
3	306,369.82	$3,827.2	$2,619.8	$211.9	$6,658.9	$16,329.4
4	309,770.52	$3,869.7	$2,648.9	$214.2	$6,732.8	$16,510.6
5	313,208.98	$3,912.6	$2,678.3	$216.6	$6,807.5	$16,693.9
6	316,685.60	$3,956.0	$2,708.0	$219.0	$6,883.1	$16,879.2
7	320,200.81	$3,999.9	$2,738.1	$221.5	$6,959.5	$17,066.6
8	323,755.04	$4,044.3	$2,768.5	$223.9	$7,036.8	$17,256.0
9	327,348.72	$4,089.2	$2,799.2	$226.4	$7,114.9	$17,447.6
10	330,982.29	$4,134.6	$2,830.3	$228.9	$7,193.8	$17,641.2
Total		**$39,362.4**	**$26,944.9**	**$2,179.3**	**$68,486.6**	**$167,947.5**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed Formulas with X_{yn-1} in year one are equal to the initial value of X_{y1}

Table 3-117: Sensitivity Training Plan Costs for Pipeline ($ Thousands)

Year	Pipeline Initial Submissions	Total Sensitivity Training Plan Cost	Total Primary Training Plan Cost
	a = a_{Y1}	b = (20% × a × 0 hours × $118.09) + (50% × a × 16 hours × $118.09) + (30% × a × 80 hours × $118.09)	c = Table 3-68
1	115.00	$434.6	$1,086.4
2	-	$0.0	$0.0
3	-	$0.0	$0.0
4	-	$0.0	$0.0
5	-	$0.0	$0.0
6	-	$0.0	$0.0
7	-	$0.0	$0.0
8	-	$0.0	$0.0
9	-	$0.0	$0.0
10	-	$0.0	$0.0
Total		**$434.6**	**$1,086.4**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed. Formulas with X_{yn-1} in year one are equal to the initial value of X_{y1}.

Table 3-118: Sensitivity Training Participation Costs for Pipeline ($ Thousands)

Year	Pipeline Training Population	General Training Cost	Privileged User Training Cost	Training Recordkeeping Cost	Total Sensitivity Training Cost	Total Primary Training Cost
	a = Column g, Table 2-2	b = (20% × a × 0 hours × $69.32) + (50% × a × .20 hours × $69.32) + (30% × a × 1.00 hours × $69.32)	c = (20% × a 15% × 0 hours × $67.44) + (50% × a 15% × .40 hours × $67.44) + (30% × a 15% × 2.00 hours × $67.44)	d = (a + (a × 15%)) × 0.02 hours × $40.63	e = b + c + d	e = Table 3-69
1	39,920.00	$1,106.9	$323.1	$37.3	$1,467.3	$3,612.2
2	40,167.50	$1,113.8	$325.1	$37.5	$1,476.4	$3,634.6
3	40,416.54	$1,120.7	$327.1	$37.8	$1,485.5	$3,657.2
4	40,667.13	$1,127.6	$329.1	$38.0	$1,494.7	$3,679.8
5	40,919.26	$1,134.6	$331.2	$38.2	$1,504.0	$3,702.6
6	41,172.96	$1,141.6	$333.2	$38.5	$1,513.3	$3,725.6
7	41,428.23	$1,148.7	$335.3	$38.7	$1,522.7	$3,748.7
8	41,685.09	$1,155.8	$337.3	$39.0	$1,532.1	$3,771.9
9	41,943.54	$1,163.0	$339.4	$39.2	$1,541.6	$3,795.3
10	42,203.59	$1,170.2	$341.5	$39.4	$1,551.2	$3,818.9
Total		**$11,383.0**	**$3,322.3**	**$383.6**	**$15,088.9**	**$37,146.9**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed Formulas with X_{yn-1} in year one are equal to the initial value of X_{y1}

Based on these altered training assumptions, under the sensitivity analysis the costs to freight rail would be $59.4 million less (59 percent reduction in cost); to PTPR would be $99.7 million less (59 percent reduction in cost); and to pipeline would be $22.7 million less (59 percent reduction

in cost). In total, the training costs under the sensitivity analysis to industry are $181.8 million less than the primary analysis.

3.8.4 Summary of Sensitivity Analysis Costs

Using this sensitivity analysis, TSA projects a possibility of what the overall costs of the proposed rule may be taking into account existing industry practices and greater variability in the methods used by covered entities to comply with the rulemaking for the largest cost drivers of the proposed rule. The following tables present the overall cost of the proposed rule by mode based upon the sensitivity analysis costs described above.

The estimated total cost to freight rail is $655.5 million which represents a 33 percent ($342.2 million) reduction from the freight rail estimated cost in the primary analysis. The total cost to PTPR 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. Finally, 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 3-119: Total Sensitivity Costs, Freight Rail ($ 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	$33,149.3	$6,664.5	$4,259.4	$22,069.2	$66,142.4	$97,652.0	-$31,509.6
2	$33,288.5	$6,869.7	$3,981.5	$19,988.6	$64,128.3	$95,471.4	-$31,343.0
3	$33,428.3	$7,080.8	$3,998.2	$18,491.5	$62,998.8	$94,622.4	-$31,623.6
4	$33,568.7	$7,298.9	$4,015.0	$20,209.7	$65,092.3	$97,002.7	-$31,910.4
5	$33,709.7	$7,524.4	$4,031.9	$18,717.7	$63,983.7	$96,187.3	-$32,203.7
6	$33,851.3	$7,756.3	$4,048.8	$20,516.0	$66,172.4	$98,675.1	-$32,502.7
7	$33,993.5	$7,995.0	$4,065.8	$19,023.4	$65,077.7	$97,885.3	-$32,807.6
8	$34,136.2	$8,241.6	$4,082.9	$20,824.7	$67,285.5	$100,405.1	-$33,119.6
9	$34,279.6	$8,495.4	$4,100.1	$19,334.9	$66,209.9	$99,647.7	-$33,437.8
10	$34,423.6	$8,757.5	$4,117.3	$21,138.6	$68,437.1	$102,200.5	-$33,763.4
Total	**$337,828.8**	**$76,684.1**	**$40,701.0**	**$200,314.2**	**$655,528.1**	**$979,749.6**	**-$324,221.5**

Note: Totals may not add due to rounding.

Table 3-120: Total Sensitivity Costs, PTPR ($ 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	$3,103.6	$6,628.6	$9,433.0	$74,602.5	$119,996.3	-$45,393.8
2	$56,052.7	$3,243.5	$6,588.3	$8,936.0	$74,820.5	$120,633.3	-$45,812.8
3	$56,674.9	$3,391.0	$6,661.5	$8,368.0	$75,095.4	$121,507.8	-$46,412.5
4	$57,304.0	$3,543.5	$6,735.4	$9,278.5	$76,861.4	$123,882.8	-$47,021.4
5	$57,940.1	$3,704.3	$6,810.2	$8,716.8	$77,171.4	$124,813.9	-$47,642.5
6	$58,583.2	$3,871.6	$6,885.8	$9,673.8	$79,014.4	$127,288.7	-$48,274.3
7	$59,233.5	$4,046.7	$6,962.3	$9,118.9	$79,361.3	$128,279.4	-$48,918.1
8	$59,891.0	$4,229.9	$7,039.6	$10,086.0	$81,246.5	$130,820.6	-$49,574.1
9	$60,555.7	$4,420.5	$7,117.8	$9,538.2	$81,632.2	$131,873.8	-$50,241.6
10	$61,227.9	$4,621.0	$7,196.9	$10,515.3	$83,561.1	$134,484.0	-$50,923.0
Total	**$582,900.2**	**$38,175.5**	**$68,626.5**	**$93,664.5**	**$783,366.7**	**$1,263,580.7**	**-$480,214.0**

Note: Totals may not add due to rounding.

Table 3-121: Total Sensitivity Costs, Pipeline ($ 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	$14,200.6	$10,494.2	$1,901.8	$38,299.3	$64,895.9	$85,636.2	-$20,740.3
2	$14,288.7	$10,733.6	$1,476.4	$35,184.8	$61,683.4	$81,122.2	-$19,438.8
3	$14,377.3	$10,978.4	$1,485.5	$32,585.2	$59,426.4	$79,132.0	-$19,705.6
4	$14,466.4	$11,228.9	$1,494.7	$35,065.0	$62,255.0	$82,232.4	-$19,977.4
5	$14,556.1	$11,485.2	$1,504.0	$32,465.4	$60,010.6	$80,265.1	-$20,254.5
6	$14,646.3	$11,747.3	$1,513.3	$35,065.0	$62,971.9	$83,508.6	-$20,536.7
7	$14,737.1	$12,015.4	$1,522.7	$32,465.4	$60,740.7	$81,564.9	-$20,824.2
8	$14,828.5	$12,289.8	$1,532.1	$35,065.0	$63,715.5	$84,832.8	-$21,117.3
9	$14,920.4	$12,570.5	$1,541.6	$32,465.4	$61,498.0	$82,913.9	-$21,415.9
10	$15,013.0	$12,857.6	$1,551.2	$35,065.0	$64,486.7	$86,207.0	-$21,720.3
Total	**$146,034.4**	**$116,400.7**	**$15,523.5**	**$343,725.5**	**$621,684.1**	**$827,415.1**	**-$205,731.0**

Note: Totals may not add due to rounding.

Table 3-122: Total Costs Under the Sensitivity Analysis ($ Thousands)

Year	Total Regulated Industries Cost	TSA Cost	Total Proposed Rule Cost		
			c = a + b		
	a	b	Undiscounted	Discounted at 3%	Discounted at 7%
1	$205,829.3	$4,426.4	$210,255.8	$204,131.82	$196,500.72
2	$200,172.1	$2,407.7	$202,579.8	$190,950.9	$176,941.0
3	$196,590.0	$2,412.2	$199,002.2	$182,115.2	$162,445.1
4	$202,803.1	$1,358.2	$204,161.4	$181,394.7	$155,753.7
5	$199,280.4	$1,363.0	$200,643.4	$173,076.7	$143,055.9
6	$205,789.1	$1,367.6	$207,156.7	$173,490.4	$138,037.2
7	$202,320.9	$1,372.3	$203,693.3	$165,621.3	$126,849.9
8	$208,895.0	$1,377.2	$210,272.2	$165,990.8	$122,380.3
9	$205,488.9	$1,382.0	$206,870.9	$158,549.3	$112,524.1
10	$212,130.2	$1,387.1	$213,517.3	$158,876.9	$108,541.4
Total	**$2,039,299.0**	**$18,853.8**	**$2,058,152.8**	**$1,754,198.1**	**$1,443,029.4**
Annualized				**$205,645.5**	**$205,454.9**

Note: Totals may not add due to rounding.

As shown in Table 3-122, the total costs to industry under the sensitivity analysis resulting from the altered assumptions discussed above are projected to be $2.1 billion. The difference from the primary analysis, which estimates a cost of $3.1 billion as presented in Column C of Table 3-94, is approximately $1.0 billion (33 percent reduction in cost from the primary analysis).

4 BENEFITS

The primary benefit of the CRM program is a possible reduction in the risk of a successful cybersecurity-incident as well as the impact of such an incident. Requirements of the proposed rule could help enhance the security of the regulated population which would reduce the chance of negative consequences and service interruptions from cyber-incidents for surface modes like freight railroad, passenger railroad, and pipelines thereby benefiting owners/operators, passengers, and consumers. The background in Section 1 of this document, and the rule's preamble, present a thorough discussion of the need for cybersecurity. This Section presents a qualitative discussion of potential benefits derived from the rule in addition to presenting a break-even analysis that helps frame the relationship between the potential benefits of the rulemaking and the costs of implementing the rule.

4.1 Qualitative Benefits

The proposed rule includes cybersecurity risk management program requirements for freight railroad, passenger railroad, and pipelines that could create benefits through the identification, protection, detection, response, and recovery from cybersecurity threats. Such potential benefits are difficult to quantify given the wide range of applicable entities with varying levels of complexity and specialized operational technology (OT) equipment, ever-changing IT systems, and uncertainty surrounding how frequent cybersecurity threats or incidents may occur and through what mechanisms. As a result, TSA identifies qualitative benefits associated with each provision that describe how the proposed cybersecurity measure may enhance security. TSA notes that the provisions in this proposed rulemaking generally align with the recommendations detailed in CISA's CPGs. As detailed in their March 2023 Update, each CPG details the risk

addressed, security action(s) that should be taken, and the resulting outcome.[366] For instance, a CPG indicates an entity should have organizational cybersecurity leadership which will address a lack of sufficient cybersecurity accountability, investment, or effectiveness. The outcome of this CPG is that a single leader is responsible and accountable for cybersecurity within an organization. This CPG aligns with the requirement in this proposal for each affected owner/operator to designate an Accountable Executive and TSA expects a similar outcome would result from having an individual with this designation and responsibility. TSA requests comment on the qualitative benefits discussed in this section.

4.1.1 Conduct a Cybersecurity Evaluation (CSE)

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[367] and physical security controls as required by proposed Sections § 1580.305, § 1582.205, and § 1586.205 of the rulemaking. The initial evaluation would identify current security vulnerabilities and areas where cybersecurity readiness could be improved. The complete enterprise-wide profile, including physical and logical/virtual controls, captures all aspects of the owner/operator and serves as a starting point to build out a larger CRM program. Recurrent evaluations can incorporate improvements, help inform prioritization, and capture new threats and vulnerabilities. Specifically, understanding and monitoring one's cybersecurity profile over time provides benefits by focusing attention on cybersecurity,

---

[366] See CISA CPG Cross-Sector Cybersecurity Performance Goals March 2023 Update at https://www.cisa.gov/sites/default/files/2023-03/CISA_CPG_REPORT_v1.0.1_FINAL.pdf. Accessed on July 24, 2024.

[367] For purposes of this analysis, logical/virtual relates to the software-based techniques as they relate to authentication, that include but are not limited to usernames and passwords, two-way authentication, and token security while physical security relates to the protection of equipment and sites from natural disasters, vandalism, and other types of damage.

providing a means to evaluate cyber related threats and mitigation measures put in place, prioritizing responses and investment to address threats and vulnerabilities where they will have the most effect, and informing budgeting for upgrade cycles and longer term investments.

4.1.2 Develop and Implement a Cybersecurity Operational Implementation Plan (COIP)

A Cybersecurity Operational Implementation Plan (COIP), as required by proposed in Sections § 1580.307, § 1582.207, and § 1586.207, helps to outline an owner/operator's strategy to address cybersecurity and describes how mitigation measures and activities will function. Documenting the operational implementation of a cybersecurity risk management program helps identify key infrastructure, establish accountability, and plan efforts to both detect threats and improve response and recovery efforts. The COIP includes several elements where the planning, effort to develop, and actual implementation could make it more likely for an owner/operator to protect and defend its network from attacks. A COIP includes governance of the CRM program, identification of critical cybersecurity systems, protection of cybersecurity systems, detection of cybersecurity incidents, and response and recovery whose specific benefits are described in more detail below. The COIP may also include a plan of action and milestones that indicates how the owner intends to implement policies, procedures, measures, or capabilities to meet plan requirements not fully in compliance, a timeframe for full compliance, not to exceed three years, and security controls necessary to achieve identified security outcomes.

4.1.3 Governance of the CRM program

This requirement, as required by proposed in Sections § 1580.309, § 1582.209, and § 1586.209, is an enabler of all the other provisions of the COIP. Effective governance of the plan could promote its successful implementation, relevance, and ability to address cybersecurity matters. This provision requires entities to identify an accountable executive and designate a

cybersecurity coordinator which are described below.

Identification of Accountable Executive

The identification of an accountable executive, as required by proposed in Sections § 1580.309(a), § 1582.209(a), and § 1586.209(a) of the rule text, requires entities to designate and notify TSA of an individual who has the knowledge and authority necessary to develop, implement, and oversee the CRM program. Identification of an executive provides authority, legitimacy, and the ability to take quick and decisive action in the event of an incident. An accountable executive responsible for cybersecurity has an incentive to improve cybersecurity. Identification of this role helps tie cybersecurity performance to this individual which encourages them to advocate and work towards adequate cybersecurity measures. Having an executive response for cybersecurity helps ensure owner/operators have a clear line of authority from which to pursue strategic objectives, align cybersecurity policy to applicable Federal standards, as well as manage and oversee execution of the CRM program. An Accountable Executive may also serve as a central point of contact or clearinghouse for cybersecurity related issues within the context of the larger organization.

4.1.4 Designation of a Cybersecurity Coordinator

Designating a cybersecurity coordinator and alternate, as required by proposed Sections § 1580.311, § 1582.211, and § 1586.211 of the rule text, improves cyber security in two ways. First, a coordinator is anticipated to be someone knowledgeable about the owner/operator's systems and who can perform the relevant coordination functions internally and externally effectively. The cybersecurity coordinator would have access to internal procedures and protocols and the relevant information about system architecture, and other vulnerabilities that

will assist that individual in responding to an incident, should one occur, and facilitate implementation of the other aspects of the proposed rule. Second, designation of a coordinator would make it easier for TSA and others to distribute cybersecurity information (e.g., threat information) and coordinate response with an owner/operator should an incident occur. Having a designated point of contact for an owner/operator and being able to reach them in a timely fashion during an incident could increase response time and potentially lessen the effects of a cyber-incident.

4.1.4.1 Identify Critical Cybersecurity Systems

Identifying critical cybersecurity systems, as required by proposed Sections 1580.313, 1582.213, and 1586.213 of the rule text, provides an understanding (or map) of what an owner/operator's system includes (e.g., points of access) and their importance to the system which allows one to determine the level of protection necessary (e.g., controlling access points). For example, identifying critical interfaces between IT and OT helps to better identify areas to protect to make them less of a target for threat actors and adversaries. Understanding what is critical is a key step in building the operational implementation plan to hone in on key dangers and optimize efforts.

4.1.4.2 Establish and Maintain Supply Chain Risk Management

There is risk imbedded in IT supply chains, and owner/operators relying on external IT and other products for the operation of their own internal IT and OT could be impacted by that risk. For example, agents of the Russian foreign intelligence service (SVR) perpetrated an attack on U.S. government entities through Microsoft products and SolarWinds in 2020. More recently threat actors breached Accellion, a secure File Transfer Protocol (FTP) site provider, in 2021. Supply chain risk management, as required by Sections 1580.315, 1582.215, and 1586.215 of the rule text, requires vendors or service providers to notify owner/operators of potential risks or

vulnerabilities which gives owner/operators the chance to develop mitigation plans or patch the identified vulnerabilities. Knowledge of risks allows recipients to reduce or mitigate the risk and encourages protection and secure movement of items along the supply chain. This relates to cybersecurity specifically by allowing entities to reduce their risk of exposure to known vulnerabilities and protect their proprietary information. This requirement encourages supply chain risk management through future procurement documents that could include options to evaluate cybersecurity measures as part of the goods or services rendered. This additional allowance in the procurement process also encourages vendors and service providers to prioritize cybersecurity as part of their standard package further enhancing the ability for owner/operators to prevent or deter future attacks.

4.1.4.3 Protect Critical Cybersecurity Systems

The establishment of policies and procedures to protect critical cybersecurity systems such as access control and IT patching, as required by proposed Sections 1580.317, 1582.217, and 1586.217 of the rule text, could help entities effectively deter, protect, and defend against incidents or make the severity of such incidents lower and the recovery time shorter.

This provision includes a number of actions that could protect entities' networks from attack, such as network segmentation that provides stop gaps or boundaries between systems and allows for higher security of more critical data, minimizing unnecessary network traffic across zone boundaries as well as securing and defending network zone boundaries which reduces the opportunity for threat actors to launch an attack.

Controlling access to Critical Cyber Systems, through multi-factor authentication for example, could make it easier to verify that network users are trusted and belong on the network. This

would reduce the potential for unauthorized access or access by threat actors. It also provides the owner/operator greater control over which internal points network users can access, creating compartments and potentially limiting unnecessary access.

Reducing risk through a patch management strategy, especially for critical systems, helps ensure systems are up to date and free from known exploits which could provide increased network security. Furthermore, a patching strategy allows owner/operators to shorten their network downtimes to ensure more reliable uptime supporting operations. For instance, a large system or a network with interconnected systems may require some time to be taken offline and de-conflicted from each other's dependencies. A patch strategy that implements isolated patching in a sandbox/testing environment before deploying them on the production system/network during a scheduled maintenance window will ensure the patches do not impact production capabilities/safety and minimize downtime.

Ensuring data is logged and establishing monitoring and logging policies gives owner/operators greater tracking of key system communications and enhances owner/operator detection and tracking/tracing capabilities as well as incident reporting accuracy and timeliness that can help stop a threat more quickly and aid recovery by identifying what was impacted.

Ensuring data is backed up and secured provides a safety net and enables faster recovery and avoids loss of critical information. Having backups of data aids in the effectiveness and institutional memory of the owner/operator's organization. If an owner/operator's network suffered a data loss it could increase their costs of doing business or cause the loss of valuable business information. Having critical system data backups mitigates this risk.

4.1.5 Cybersecurity Training and Knowledge

This provision, as required by proposed Sections § 1580.319, § 1582.219, and § 1586.219 of the rule text includes cybersecurity training program requirements for employees, curriculum requirements, and retention of training records. This includes both basic cybersecurity training and role based or privileged user training.

Training could strengthen cybersecurity knowledge among all owner/operator employees thus making them less susceptible to threats and more prepared to take action when threats occur. IBM's 2023, "Cost of a Data Breach," report indicates that employee training and knowledge is a key driver to reducing the consequence magnitude of a data breach.[368] Additionally, more than 50 percent of organizations which suffer a breach invest more in additional employee training following a breach. While employee training may not be fully effective, or change the probability of an attack, IBM's report suggests that it is associated with lower consequence magnitudes.[369] Privileged user employees would receive additional more focused training as they have greater ability to do harm and thus need to be more mindful. Frequently, breaches occur due to the actions of an individual inside an organization who may not be malicious themselves, but possibly careless or unsuspecting. For example, something as simple as clicking on a link in a suspicious email could cause harm and is a frequent tactic of threat actors. There are other ways that insiders can unknowingly grant access to external threat actors. For example, by falling victim to a social engineering scheme, such as one where the user may answer a phone call from

[368] "Cost of a Data Breach Report 2023." IBM Security. https://www.ibm.com/data_breach/2023. Accessed June 13, 2024.

[369] Furthermore, employee training, even for non-privileged users may act as a "signal" from the organization to its employees to generally take cybersecurity seriously. By convincing employees that cybersecurity is a priority, such trainings may deter risky employee behaviors on the margins.

an unknown source and is convinced by the scammer to divulge sensitive information or passwords. Thus, entities training their employees on cybersecurity could help them prevent and identify incidents through increasing the knowledge of their network users with improved understanding of cyber-hygiene best practices, acceptable use, risks associated with their level of privileged access, and awareness of security risks associated with their actions. These benefits of cybersecurity training are reinforced by CISA's Cross-Sector Cybersecurity Performance Goals (CPGS).[370] Trained individuals are less likely to engage in risky behaviors such as clicking on external links and more likely to be responsible with cybersecurity and IT infrastructure. For example, studies from the healthcare context show that when workers are trained on how to recognize phishing attacks, they are less likely to click on suspicious links.[371] Role-based training would also specifically address their role as a privileged user to prevent and respond to a cyber-incident. Both help reduce the number of successful cyber-incidents and the resulting need to respond to them, thereby increasing surface transportation network's ability to operate as expected.

4.1.6 Detect Cybersecurity Incidents

Policies, procedures, and capabilities in place that can detect cybersecurity threats and anomalies, as required by proposed Sections § 1580.321, § 1582.221, and § 1586.221 of the rule

---

[370] The latest CISA CPG includes basic cybersecurity awareness training as one of its best practices. See CISA Cross-Sector Cybersecurity Performance Goals (CPG) March 2023 Update, Detect- 3.A. Retrieved Oct. 14, 2023 from https://www.cisa.gov/sites/default/files/2023-03/CISA_CPG_REPORT_v1.0.1_FINAL.pdf.

[371] A study by KnowBe4 measured the baseline click rate for suspicious links for over 9.4 million users across 9 sectors and 300,000 organizations. KnowBe4 found that users click rates on suspicious links dropped more than 17 percent relative to baseline following training. Osterman Research found double and sometimes triple-fold increases in employee awareness of various attack vectors following training. See, McKeon, Jill. "Security Awareness and Training Crucial to Preventing Healthcare Phishing Attacks." Cybersecurity News. July 14, 2022. https://www.healthitsecurity.com/news/security-awareness-and-training-crucial-to-preventing-healthcare-phishing-attacks.

text, allow owner/operators to identify and respond to intrusions and issues more quickly and thus potentially reduce the amount of damage or harm.[372] Having an awareness of what is happening on one's network can improve defense, understanding of system weaknesses and adversaries, and coordination with others that experience similar incidents. Earlier detection of incidents through deployment of these capabilities and sharing of such information, through the reporting requirement, can help a broader set of entities suffer fewer attacks, respond more effectively if attacked, and reduce the severity and recovery time from an attack. TSA intends to leverage the reports it receives to further strengthen cybersecurity awareness and posture in the transportation sector. For instance, if a particular threat actor tries a technique and is successful in penetrating a transportation sector entity's network, it is possible they may try so again on another entity using the same vector of attack until they met resistance. While an attack, network defense, or recovery effort was ongoing, and in the absence of a reporting requirement, entities who were the victim of a known attack may be reluctant to share that information with the public or others in the sector. Sharing such information could have adverse effects on their business operations and revenue. This could result in a situation where other entities in the transportation sector could suffer the same or similar attack. Greater knowledge of attacks that have happened may spur action (e.g., similar incidents could happen to me). Similar impacts would also be attributed to other incidents. In addition, this requirement provides a means to share such information in a non-attributable way that would include a larger data set of incidents which is continuously updated.

---

[372] Knowledge of relevant threats and ability to detect them protect against threat actors that may exist undetected in their networks for long periods. CISA Cross-Sector Cybersecurity Performance Goals (CPG) March 2023 Update, Detect- 3.A. Retrieved Oct. 14, 2023 from https://www.cisa.gov/sites/default/files/2023-03/CISA_CPG_REPORT_v1.0.1_FINAL.pdf.

4.1.6.1 Respond and Recover

Proposed sections 1580.323, 1582.223, and 1586.223 would require owner/operators to incorporate abilities to respond to and recover from a cybersecurity incident into their COIP, which allows them to rapidly implement mitigation measures upon an incident as well as respond and recover faster.[373] Such actions can include auditing access to unauthorized websites or domains, documenting and auditing communications between the OT system and an external system, identifying and responding to unauthorized code execution, as well as defining, prioritizing, and standardizing incident response activities, such as security orchestration, automation, and response (SOAR).

Capabilities to respond to cybersecurity incidents

This requirement details what capabilities owner/operators must possess to be able to respond to incidents as part of their COIP. Having such capabilities in place could help owner/operators effectively respond to cybersecurity incidents thereby reducing incident impacts. Having a plan to respond to incidents is helpful, but having the tools in place enhances the effectiveness of the response plan and helps owner/operators respond and protect their critical cybersecurity systems more rapidly and thoroughly in the event of an incident. This is also consistent with the NIST CSF. Having the capabilities to respond to an incident help owner/operators mitigate the severity of an incident should one occur and likely reduce the time spent out of operation as well as mitigate damage to any affected critical systems. Specifically, this requirement helps ensure

---

[373] Mitigates against the inability to quickly and effectively contain, mitigate, and communicate about cybersecurity incidents. Incident planning and preparedness improves organizations capability of safely and effectively recovering from a cybersecurity incident thus avoiding or reducing disruption to availability of an asset, service, or system. CISA Cross-Sector Cybersecurity Performance Goals (CPG) March 2023 Update, Protect- 2.S and Recover- 5.A. Retrieved Oct. 14, 2023 from https://www.cisa.gov/sites/default/files/2023-03/CISA_CPG_REPORT_v1.0.1_FINAL.pdf.

owner/operators already have the tools at their disposal to respond to an incident more rapidly than if an owner/operator had to spend time acquiring or developing the capabilities to respond while an incident is ongoing.[374] For those without or with limited capabilities, this requirement would elevate such capabilities and thus improve the capability to respond to a cybersecurity incident.

4.1.7 Reporting of Cybersecurity Incidents

Proposed sections 1580.326, 1582.225, and 1586.225 would require owner/operators to report cybersecurity incidents within 24 hours after a cybersecurity incident is identified. As reporting cybersecurity incidents is a requirement of the proposed rule, failure to make a timely report could result in civil penalties for non-compliance. Reporting incidents to CISA allows owner/operators to access the immediate support of TSA and CISA cybersecurity experts during incident response and recovery. Agency experts may have specific knowledge useful in the mitigation or resolution of the incident from experience related to other owner/operators. Such assistance could lessen the severity of an incident on an owner/operator's systems and shorten its recovery time to full operation. Timely incident reporting can provide critical insight into the broader threat landscape; such as whether an attack is isolated or a broader attack against the sector.[375] In addition, other surface transportation owner/operators, and in turn the public, benefit from TSA and CISA seeing how threat actors were able to breach the affected owner/operator and use this information to forewarn other regulated entities about such threat actor tactics. TSA and CISA will keep detailed records of reported incidents and be able to use the reported incident

[374] For those owner/operators without or with limited capabilities, this requirement would elevate such capabilities and thus improve their capability to respond to a cybersecurity incident.

[375] CISA Cross-Sector Cybersecurity Performance Goals (CPG) March 2023 Update, Respond - 4.A. Retrieved Oct. 14, 2023 from https://www.cisa.gov/sites/default/files/2023-03/CISA_CPG_REPORT_v1.0.1_FINAL.pdf.

to identify trends, assist in the response, and try to help mitigate any broader impacts of the incident to the larger economy. Each incident report would be processed through TSA's Transportation Security Operations Center (TSOC) for analysis by watch officers, and other specialists to identify potential trends. TSA would then share timely information with the field to notify them of emerging potential threats to relevant to surface stakeholders. For example, if a freight railroad cybersecurity breach will affect rail traffic through a key interchange, and TSA is alerted to the incident, TSA could assist other operators in avoiding the affected owner/operator's trackage while incident response and recovery is underway, thereby keeping overall transportation systems operable.

4.1.8 Cybersecurity Incident Response Plan (CIRP)

Each owner/operator required to have a CRM program must have an up-to-date CIRP for their Critical Systems, as required by proposed § 1580.327, § 1582.227, and § 1586.227 of the rule text. A CIRP must provide specific measures to ensure identification, isolation, and segregation of the infected systems from the uninfected systems, secured backed-up data stored offline, and capability and governance for implementing mitigation measures to keep the OT system separate from the IT system.

By requiring an established set of policies and procedures in place to respond to intrusions into their critical cybersecurity systems, entities could benefit from a reduction in time and confusion with how they respond to future incidents.[376] They may also be able to lessen service

[376] IBM releases an annual research report on the Cost of a Data Breach. IBM's two most recent reports, from 2023 and 2022, show that investment in certain types of cybersecurity measures are associated with lower consequence magnitudes for data breaches that do occur. Specifically, the report notes that those organizations sampled which had an Incident Response plan in place were able to contain incidents on average 54 days faster than those with

interruptions by having alternative plans that can be used and utilize built-in redundancies. Without a plan, an owner/operator may spend valuable time trying to decide what to do next. Having a CIRP in place could enable faster response as well as lowering the severity and reducing recovery time of successful attacks. A CIRP could allow an owner/operator to more accurately and quickly notify its customers and stakeholders of an emerging incident, which systems and processes it will and will not affect, and how likely and quickly they are to be back online. Setting these expectations with customers and suppliers could help to build and maintain trust in an organization.

4.1.9 Cybersecurity Assessment Plan (CAP)

Owner/operators must submit a plan to annually assess the CRM program, as identified in § 1580.329, § 1582.229, and § 1586.229 of the rule text. The assessment looks at the execution of one's COIP, effectiveness of mitigation measures implemented, and assessment of continued vulnerabilities. The potential benefit of the assessment plan is the accountability created through the annual report that evaluates the effectiveness of one's CRM program by indicating if the provisions outlined in the COIP are being followed, assessing the performance or effectiveness of measures taken (e.g. through penetration testing, coverage of access management such as MFA, and patch management), and comparing those defenses against identified vulnerabilities. In addition, highlights of the CAP that provide accountability include the bi-annual architectural design review (ADR), other assessments designed to identify vulnerabilities to critical systems,

---

neither an Incident Response team or plan. "Cost of a Data Breach Report 2023." IBM Security. https://www.ibm.com/data_breach/2023. See also, "Cost of a Data Breach Report 2022." IBM Security. https://www.key4biz.it/wp-content/uploads/2022/07/Cost-of-a-Data-Breach-Full-Report-2022.pdf.

CISA also encourages agencies and entities to use its assessment tool and vulnerability scanning to reduce exposure to exploits and other exploitable internet services. See https://www.cisa.gov/news-events/news/cybersecurity-performance-goals-assessing-how-cpgs-help-organizations-reduce-cyber-risk.

auditors independent from individuals who have oversight or responsibility for implementing the owner/operators CRM program, and the requirement to transparently report these results to TSA and corporate leadership. The ADR provides benefit to owner/operators through the verification of network traffic and ensuring the network design and interconnectivity stay up to date and secure. The other assessments could benefit owner/operators by highlighting their vulnerabilities, the nature of potential exploits, and a roadmap for how to fix such vulnerabilities so that they cannot be exploited in a cybersecurity incident. The independent assessors and auditors could supplement the internal efforts by entities by providing an independent and external assessment of cybersecurity vulnerabilities without the potential for being motivated by internal incentives. The reporting of the results from the ADR and auditing help hold the owner/operators accountable for maintaining a strong CRM program and facilitate continual improvement thereby limiting the impact of future threats or incidents on surface transportation infrastructure.

4.1.10 Documentation

This provision, as required by proposed § 1580.331, § 1582.231, and § 1586.231 of the rule text, lists a series of documentation an owner/operator must maintain to demonstrate compliance with the CRM requirements. The benefit of such documentation is a simpler and more clearly understood process to establish compliance. Documentation is a necessary requirement for verifying compliance with the rule's requirements as documents provide a record of plans, policies, procedures, training, etc. Requiring retention of certain documents necessary to establish compliance, as well as TSA's right to review all documents related to compliance, is authorized under 49 U.S.C. 114(f). It creates a level of expectation between the government and owner/operators regarding what documentation needs to be retained and made available. This reduces the time spent in compliance inspections, encourages consistency, and helps ensure

owner/operators and TSA are on the same page. As a result, TSA would be able to better enforce and administer the rule and thus reap the benefits of its provisions.

4.1.11 Physical Security Requirements

The proposed requirements in Sections 1586.103 and 1586.105 of the rule text, add additional requirements related to the physical security portion of the pipeline security program. The benefit of requiring pipeline owner/operators to have designated security coordinators and report significant security concerns is to help facilitate communication. Reporting security incidents and concerns increases TSA's capability to analyze potential threats, understand the industry landscape, and take appropriate action to help reduce threat. Security coordinators provide TSA a designated point of contact to communicate security threats and other important information with someone in a position to disseminate such information appropriately.

4.1.12 TSA Oversight

Under the proposed rule, TSA would review each entity's CSE, CIRP, CAP, and COIP. Review of these documents helps hold owner/operators accountable and enables TSA's cyber experts and other SMEs to provide guidance and support to help entities create or select appropriate and effective policies, approaches, or actions based on their size and operations.

4.2 Marginal Benefit Analysis

Table 4-1 below summarizes the qualitative benefits of each proposed rule requirement alongside their associated annualized cost at seven percent.

Table 4-1: Total Ten-Year Costs of the Proposed Rule by Requirement with Qualitative Benefits

NPRM Requirements	49 CFR	Annualized Costs at 7% (% of Total)	Description	Benefits
Cybersecurity Evaluation (CSE)	§ 1580.305 § 1582.205 § 1586.205	$1,399.6 (0.5%)	Owner/operators are expected to evaluate and create a current profile of CRM program including both physical and logical/virtual security controls.	Provides a high level overview of entities current status that identifies cyber vulnerabilities, gaps, remediation, and mitigation measures, informs prioritization of response actions and investment to address threats and vulnerabilities, and can support budgeting for upgrade cycles and longer term investments.
Cybersecurity Operational Implementation Plan (COIP)	§ 1580.307 § 1582.207 § 1586.207	Costs are captured under requirements below	Require owner/operators to detail their defense-in-depth plan, including physical and logical/virtual security controls, to comply with the requirements and how the owner/operator meets these requirements for governance, identification of critical systems, protection of critical systems, detection and response of incidents.	Benefits are captured under each COIP requirement (Governance of the CRM, Cybersecurity Coordinator, Identification of Critical Cyber Systems, and Supply Chain Risk Management) below. However, there is also an overall benefit of having a plan and going through the planning process.
Governance of the CRM	§ 1580.309 § 1582.209 § 1586.209	$1,637.6 (0.5%)	Each owner/operator must identify an Accountable Executive and keep this information updated with TSA. 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. The COIP must also include identification of positions designated to manage implementation of policies and procedures and any authorized representatives responsible for implementation and oversight of the CRM.	Identification of an accountable executive ties cybersecurity performance to an individual, fostering a clear line of authority from which to pursue strategic objectives, align cybersecurity policy to applicable Federal standards, as well as manage and oversee execution of the CRM program.
Cybersecurity Coordinator	§ 1580.311 § 1582.211 § 1586.211	$41.3 (0.0%)	Owner/operators are required to designate a cybersecurity coordinator who is required to be available to TSA and DHS's Cybersecurity and Infrastructure Security Agency (CISA) at all times (all hours/all days) to coordinate cybersecurity and address any incidents that arise.	Establishes a point of contact with knowledge of internal systems, protocols, and vulnerabilities for owner/operators in the event of an incident for cyber related activities and to receive and implement information provided by TSA or CISA (e.g. alerts related to cyber incidents).

NPRM Requirements	49 CFR	Annualized Costs at 7% (% of Total)	Description	Benefits
Identification of Critical Cyber Systems	§ 1580.313 § 1582.213 § 1586.213	$1,184.2 (0.4%)	Owner/operators must identify Critical Cyber Systems including the identifying information, identification methodology, system information and network architecture, additional systems, and changes to Critical Cyber Systems.	Documents and provides an understanding of what an owner/operator's systems include (e.g., points of access), their importance, use, dependencies, and potential vulnerabilities, which informs necessary levels of protection and access.
Supply Chain Risk Management	§ 1580.315 § 1582.215 § 1586.215	$7,209.4 (2.3%)	Owner/operators will consider cybersecurity in all aspects of vendor and procurement agreements. Owner/operators are encouraged to select the more secure offer between two vendors of similar cost and function. All procurement documents and contracts, including service-level agreements, executed or updated after the effective date of the final rule include a requirement for vendor or service providers to notify owner/operators of cyber incidents affecting vendor or service providers and confirmed security vulnerabilities affecting the vendor service. Upon notification of a cybersecurity event or vulnerability, owner/operators must consider mitigation measures sufficient to address the resulting risk to Critical Cyber Systems and, if any of these measures would result in permanent changes, the owner/operator would need to request to amend its COIP.	Ensures that the most secure products and services are purchased and that purchasing priority is given to more secure vendors. Helps ensure owner/operators are aware of upstream supply risks or potential issues associated with products or services provided. May lead to a reduced risk of exposure to known vulnerabilities through improved and standardization of cybersecurity as part of vendor packages. Additionally, it promotes consistent cyber security practices across the supply chain, enhances overall system resilience, and supports compliance with regulatory requirements.

NPRM Requirements	49 CFR	Annualized Costs at 7% (% of Total)	Description	Benefits
Protection of Critical Cyber Systems	§ 1580.317 § 1582.217 § 1586.217	$247,567.9 (80.4%)	The owner/operator must incorporate into its COIP network segmentation and other policies, procedures, controls and capabilities to protect Critical Cyber Systems. This includes IT/OT communications, patching, ensuring logging data are secured and stored centrally, backups, and protections that control access to systems.	Encourages a systematic protection or safeguarding of systems that have the greatest potential for negative impacts (e.g., shutdown of operations). Network segmentation helps owner/operators determine appropriate protection measures based on the type of system or information and hinder intrusion efforts. Patching efforts help ensure network security. Ensuring logging data are stored in a secure and central location can prevent destruction of data that identify perpetrators and vulnerabilities, and help more quickly identify perpetrators of a cybersecurity incident. Backups enable faster recovery and can avoid the loss of critical information. Access controls enable easier verification of trusted network users and reduce potential for unauthorized or threat actors to access systems.
Cybersecurity training and knowledge	§ 1580.319 § 1582.219 § 1586.219	$30,750.8 (10.0%)	Owner/operators required to have a CRM program must provide basic cybersecurity training to all employees, including contractors, with access to the owner/operator's Information or Operational Technology systems and role-based cybersecurity training for cybersecurity-sensitive employees.	Informs employees of potential pitfalls, best practices, and potential negative impacts of cyber incidents. Increased awareness can help prevents and improve response to cyber incidents. Role-based training specific to privileged users can further support incident prevention by tailoring specific security measures and practices for roles that are at greater risk of being targeted by malicious actors, due to their access to internal systems.
Detection of cybersecurity incidents	§ 1580.321 § 1582.221 § 1586.221	$2,213.7 (0.7%)	The owner/operator must incorporate into its COIP policies, procedures, and capabilities sufficient to detect cybersecurity threats to, and anomalies on, Critical Cyber Systems.	Helps ensure cyber incidents/intrusions are discovered and quickly addressed (faster than without detection and response capabilities). Addressing such matters more quickly could limit or reduce their impact and allow for the sharing of incident information with TSA and others sooner.

NPRM Requirements	49 CFR	Annualized Costs at 7% (% of Total)	Description	Benefits
Capabilities to respond to a cybersecurity incident	§ 1580.323 § 1582.223 § 1586.223	Captured in Reporting and detection of cyber incidents	The owner/operator must incorporate into its COIP capabilities to respond to cybersecurity incidents affecting Critical Cyber Systems, including documenting and auditing any communications between OT and IT systems, responding to execution of unauthorized code, and ensuring standardized incident response activities.	Ensures more effective responses than if the owner/operator has to acquire or develop capabilities to respond while an incident is ongoing.
Reporting Cyber Incidents	§ 1580.325 § 1582.325 § 1584.107 § 1586.325	$41.6 (0.0%)	Owner/operators are required to report cybersecurity incidents to the CISA.	Shares incident information across the industry that may lessen severity of incidents by raising awareness faster to other entities and compiling trends and other insight to share across the industry. Reporting also informs TSA and CISA, whose cybersecurity experts may be able to assist during response and recovery. Timely reporting can also assist TSA in identifying if an incident is isolated or part of a larger effort on industry.
Cybersecurity Incident Response Plan (CIRP)	§ 1580.327 § 1582.227 § 1586.227	$8,668.3 (2.8%)	CIRP requirements include having a plan to ensure the impacts of a cybersecurity incident are limited and don't spread throughout the system, back-up data is tested before it is used for recovery, measures are in place to ensure isolation of technology to reduce risks, and identification of who, by position, is responsible for implementing measures in the plan. TSA would continue to require owner/operators to test their plans through exercises and modify the CIRP based on the results of the exercises.	Allows for faster response, lowered severity or impact, and decreased recovery time following successful incidents. Can allow for more accurate and faster notification to customers and stakeholders that may help build and maintain trust in the organization.

NPRM Requirements	49 CFR	Annualized Costs at 7% (% of Total)	Description	Benefits
Cybersecurity Assessment Plan (CAP)	§ 1580.329 § 1582.229 § 1586.229	$5,729.0 (1.9%)	The CAP includes cybersecurity architecture design review and also requires owner/operators to use other assessment capabilities intended to test the effectiveness of their cybersecurity measures. The CAP must include a specific schedule for the assessments to ensure that at least 30 percent of the COIP is tested each year, and at a pace to ensure 100 percent is tested every three years.	Regular testing of cybersecurity measures allows for identification of vulnerabilities and potential pitfalls, allowing for remediation prior to a potential incident that takes advantage of those vulnerabilities. The CAP also creates accountability among owner/operators by compelling this regular review and assessment of their cybersecurity measures and facilitates continual improvement. The biannual architecture design review requires owner/operators to verify and validate their network traffic and ensure network design and interconnectivity are up to date and secure. Independent audits provide an objective assessment of cybersecurity vulnerabilities. Ensuring that at least 30 percent of the COIP is tested each year spreads out the burden of these requirements while ensuring cybersecurity remains a consistent priority. A standardized plan allows for owner/operators to develop scalable and adaptable security measures. Standardized measures aid in mitigating cyber threats, reducing the risk of breaches that could disrupt the sector. A uniform approach aids in identifying vulnerabilities and addressing them proactively. Organizations can more easily integrate new technologies within a structured framework (i.e. CSF, NIST, ISO27000, etc.)
Documentation to establish compliance	§ 1580.331 § 1582.231 § 1586.231	$1,214.7 (0.4%)	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.	Fosters efficient administration and enforcement of the rule's requirements. Compelling compliance can decrease the time burden of recordkeeping and record review and improve consistency.
Physical Security Coordinator	§ 1586.103	$4.5 (0.0%)	Each owner/operator 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.	Provides a designated point of contact to whom TSA can communicate security threats and other important information. Physical security coordinators are also in a position to disseminate communications from TSA to other individuals in the operation, serving

NPRM Requirements	49 CFR	Annualized Costs at 7% (% of Total)	Description	Benefits
				as one point of contact who can convey important information on TSA's behalf to multiple key stakeholders.
Reporting of Significant Physical Security Concerns[377]	§ 1586.105	$93.9 (0.0%)	Each owner/operator must report, within 24 hours of initial discovery, any potential threats and significant physical security concerns involving transportation-related operations and other potential threats or significant physical security concerns.	Facilitates communications and increases TSA's ability to analyze potential threats. TSA's experts may be able to assist during response and recovery. Timely reporting can also assist TSA in identifying if an incident is isolated or part of a larger effort on industry.

TSA acknowledges that some of the measures put forth in this NPRM might already be implemented across industry. However, the purpose of the proposed rule is to establish a standardized cybersecurity risk management program to promote the protection of the surface transportation sector as it expands and evolves.

4.3 Break-Even Analysis

TSA includes a break-even analysis to compare the potential security benefits of the CRM Program with the costs of implementing them. When it is not possible to quantify or monetize the incremental security benefits of a regulation, OMB recommends conducting a threshold, or break-even, analysis. According to OMB Circular No. A–4, "Regulatory Analysis," such an analysis answers the question, "How small could the value of the non-quantified benefits be (or how large would the value of the non-quantified costs need to be) before the rule would yield zero net benefits?"[378] This analysis compares the full cost of the CRM program with the major

[377] As previously discussed, physical security requirements, including designation of a physical security coordinator and reporting of significant physical security concerns are already applicable to Freight Rail, PTPR, and OTRB industries under TSA's Security Training rulemaking. New costs are only associated with the Pipeline industry.

[378] Readers can access OMB Circular No. A-4 dated September 17, 2003 at, https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A4/a-4.pdf, accessed September 3, 2023.

direct consequences incurred by the types of cybersecurity incidents that could potentially be averted when these provisions are implemented. TSA uses the full cost of the CRM program in this break-even analysis without adjusting for costs industry has incurred as a result of the SDs or other previous voluntary efforts performed by industry.

Ideally, quantifying and monetizing the security effects of the CRM Program would be a two-step process. First, TSA would estimate the reduction in the probability of a successful cybersecurity attack, along with the fully quantified consequences of an incident averted by the deployment and use of the proposed cybersecurity measures. These two estimates compose the total risk associated with a potential attack. Second, to monetize the benefit, TSA would estimate the willingness of individuals to pay for this incremental risk reduction and apply that to the population experiencing the benefit.[379] However, TSA is not able to estimate the probability of a successful attack. This estimate is difficult to quantify due to the complexity and changing nature of IT, OT, and their intersection as well as both bad actors and cybersecurity protection constantly evolving to anticipate the next attack. Given this difficulty, TSA uses a break-even analysis to help inform decision makers by comparing program costs with potential benefits.

There are a wide range of events that TSA believes a CRM program can help protect against, from small incidents like targeted ransomware attacks and data breaches to large incidents like complex network attacks that threaten human life and/or take operations offline for extended periods of time.

[379] Willingness to pay measures the amount of money people would be willing to spend for a good or service, and is therefore a proxy for the contribution of that good or service to their well-being. Economists commonly seek to measure willingness to pay to estimate the benefits of a good or service to consumers.

For example, the Colorado Department of Transportation experienced a ransomware attack in February 2018 that took a month to be fully resolved. A staff of at least 25 IT professionals worked six-hour days and managed to contain the malware and restore the system. The system backup restoration continued for another three weeks.[380] At the peak of the containment effort, 150 people were working to contain the malware and begin the restoration process.[381] Reports estimate that these efforts cost the state $1.96 million in overtime, meals, and equipment. [382] Following this attack, the Colorado State Legislature passed a $13.3 million budget increase for the State's Office of Information Technology and now spends close to $20.42 million on cybersecurity.[383]

On the other end of the spectrum, CISA's report titled "Cost of a Cyber Incident: Systematic Review and Cross-Validation" discusses the costs of cybersecurity incidents in the United States that may result in extreme economic losses.[384] Although the estimates provided in the report are not specifically for cybersecurity incidents in the U.S. surface transportation industry, the report

---

[380] "How SamSam ransomware took down CDOT and how the state fought back — twice." Tamara Chuang. The Colorado Sun. February 3, 2020. Accessed September 28, 2023. https://coloradosun.com/2020/02/03/how-samsam-ransomware-took-down-cdot-and-how-the-state-fought-back-twice/.

[381] "Cyber attack on CDOT computers estimated to cost up to $1.5 million so far." Tamara Chuang. The Denver Post. April 5, 2018. Accessed September 28, 2023. https://www.denverpost.com/2018/04/05/samsam-ransomware-cdot-cost/.

[382] "How SamSam ransomware took down CDOT and how the state fought back — twice." Tamara Chuang. The Colorado Sun. February 3, 2020. Accessed September 28, 2023. https://coloradosun.com/2020/02/03/how-samsam-ransomware-took-down-cdot-and-how-the-state-fought-back-twice/. Original estimates $1.7 million, $11.9 million and $17.7 million respectively, converted to 2022 dollars.

[383] "How SamSam ransomware took down CDOT and how the state fought back — twice." Tamara Chuang. The Colorado Sun. February 3, 2020. Accessed September 28, 2023. https://coloradosun.com/2020/02/03/how-samsam-ransomware-took-down-cdot-and-how-the-state-fought-back-twice/. Original estimates $1.7 million, $11.9 million and $17.7 million respectively, converted to 2022 dollars.

[384] CISA's Cost of a Cyber Incident: Systematic Review and Cross-Validation report dated October 26, 2020, https://www.cisa.gov/sites/default/files/publications/CISA-OCE_Cost_of_Cyber_Incidents_Study-FINAL_508.pdf. The report provides aggregate annual cost estimates using different sources for cybersecurity incidents in the United States and incidents that have global impacts on pages 11 through 15. Page 11 of the report provides a range of estimates for U.S. impacts starting under $1 billion ($0.53 billion) up to $242 billion (see table 2 of the report). Report accessed September 2023.

shows that cybersecurity incidents can cause extreme economic losses into the billions of dollars and may involve downstream economic and social impacts beyond the direct business impacts to the affected entities.

A key impact of a major cybersecurity incident with regards to surface transportation is its ability to cause cascading effects that reach many aspects of the U.S. economy and daily life. An incident of this nature is likely not the result of an intrusion into a single company or pipeline but is perpetrated by an advanced well-resourced actor that is able to target multiple critical systems (e.g., data, personnel management, and/or safety systems) across a spectrum of the industry. Beyond any physical or other direct costs, disruption to the transportation industry may create supply shortages for energy supplies, finished goods, agriculture, and the ability to complete just-in-time shipments. Examples of just in time shipments include food supply to grocery stores, gas stations, and car manufacturing where a delay in parts or materials may slow or stop other aspects of the production process. Delay or disruptions that lead to energy supply shortages could also lead to increased energy costs which would then impact the costs of other goods as well. Depending on the incident, impacts may be felt regionally first, but could cascade into national or global impacts if the incident keep critical transportation systems offline.

One of the major components driving the impact from a cybersecurity incident is time or duration that the transportation system is down or operating at a reduced capacity. There is a level of resiliency and short term redundancies that would enable people and businesses to cope for a few days; but once those are exhausted, businesses may have to temporarily shut down and key commodities like gasoline may need to be rationed and prioritized for use by emergency service providers like police, fire, and ambulances to sustain essential services.

The implementation of a cybersecurity risk management program, as proposed by this rule, seeks to reduce the risk and mitigate the worst of such large scale systemic shutdowns. This is accomplished through the implementation of systems, policies, and procedures to secure essential cyber systems and the ability to effectively respond to cybersecurity incidents. Such actions would also help mitigate smaller cybersecurity incidents and thus provide additional benefits.[385]

For example, the IBM and Ponemon Institute's 2023 report on the cost of a data breach showed that organizations with an incident response plan and team had on average 5 percent lower costs to contain and recover from a breach than those which did not.[386] However, as the IBM and Ponemon Institute show, the vast majority of known data breaches result in consequence magnitudes far below those offered in the scenarios below. TSA recognizes that consequence magnitude and probability are likely inversely related, meaning that there is greater probability, all else equal, of a lower consequence cyber attack than a higher one, and lower probability of a higher consequence attack.

The following are a few examples of less significant cybersecurity incidents with lower consequence magnitudes. In 2016, the Orange County Transportation Authority was struck by a cyber attack that took control of 88 of the agency's servers.[387] The attack used ransomware and

---

[385] TSA notes that many of the actions put in place that could help address larger incidents would also help address smaller incidents. For example, having data backup could help bring a system back online following a large cyber incident as well as diminish the impact of a ransomware attack that attempts to corrupt or deny access to it.

[386] "Cost of a Data Breach Report 2022." IBM Security. https://www.key4biz.it/wp-content/uploads/2022/07/Cost-of-a-Data-Breach-Full-Report-2022.pdf.

[387] Gerda, Nick. "Transportation Authority Kept Secret Cyber Attack That Cost $600,000". August 2, 2016. Voice of OC: Orange County's Nonprofit Newsroom. https://voiceofoc.org/2016/08/transportation-authority-kept-secret-cyber-attack-that-cost-600000/.

the attackers demanded $8,500 in ransom payments. The County was able to restore its servers from the disruption at a total cost of over $600,000. More recently, May of 2024, the Washington Area Metro Transportation Authority (WMATA) experienced a Distributed Denial-of-Service (DDOS) attack on its public-facing website which shut down access for two hours.[388] WMATA's riders were not affected and SmarTrip and mobile applications were not impacted. WMATA has yet to publicly share a cost impact of the attack, but the scope and duration of the attack, and WMATA's report that no customer or employee data was compromised point to a relatively low consequence magnitude of the attack.

The break-even analysis inputs and scenarios presented below are chosen to provide the reader with an understanding of the potential impacts of successful cyber attacks. The selection of these scenarios and consequence magnitudes does not express TSA's opinion that such attacks are likely to occur, or even more likely than attacks of other smaller magnitudes. These hypothetical scenarios are meant to illustrate the plausibility of the rule breaking even, or having no net cost impact on the regulated entities. However, it also does not account for the possible cumulative avoided consequence of many smaller events that the rule could help prevent or mitigate. TSA requests comment on the inputs and scenarios discussed in the subsequent sections.

4.3.1 Break-Even Analysis Inputs

As part of calculating the break-even point of an analysis, TSA uses the full cost of the CRM program and cybersecurity related costs to assess the level of benefits or avoided costs required

[388] Anderson, Amber. "Metro experiences cybersecurity attack, website shut down for hours". May 14, 2024. WUSA9 News. https://www.wusa9.com/article/traffic/mission-metro/metro-experiences-cybersecurity-attack-website-shut-down-for-hours-denial-of-service/65-3d3ce5ba-21b2-4d6e-804f-52e83411378d.

to break even.[389] Table 4-2 shows total cybersecurity risk management costs attributable to TSA by regulated modes for the modes that are creating CRM programs. It does not include OTRB or pipeline physical security related costs. These TSA costs are summarized in Section 3.5.6 in a different format, but presented here by regulated mode. These costs include TSA operating costs to review and approve documents submitted by regulated entities. It displays the total TSA cost using a seven percent discount rate.

Table 4-2 TSA Cybersecurity Risk Management Costs by Regulated Mode ($ Thousands)

Year	Industry			Total TSA Cost		
	Freight Rail	PTPR	Pipeline	d = ∑a,b,c		
	a	b	c	Undiscounted	Discounted at 3%	Discounted at 7%
1	$1,369.7	$642.8	$2,339.0	$4,351.5	$4,224.7	$4,066.8
2	$704.4	$339.0	$1,289.3	$2,332.7	$2,198.8	$2,037.5
3	$706.2	$341.7	$1,289.3	$2,337.2	$2,138.9	$1,907.9
4	$360.1	$182.2	$741.0	$1,283.3	$1,140.2	$979.0
5	$362.0	$185.0	$741.0	$1,288.0	$1,111.1	$918.4
6	$363.9	$187.7	$741.0	$1,292.6	$1,082.6	$861.3
7	$365.8	$190.6	$741.0	$1,297.4	$1,054.9	$807.9
8	$367.7	$193.5	$741.0	$1,302.3	$1,028.0	$757.9
9	$369.7	$196.4	$741.0	$1,307.1	$1,001.8	$711.0
10	$371.6	$199.5	$741.0	$1,312.2	$976.4	$667.0
Total	**$5,341.2**	**$2,658.4**	**$10,104.7**	**$18,104.3**	**$15,957.3**	**$13,714.7**
Annualized					**$1,870.7**	**$1,952.7**

Table 4-3 shows the combined TSA and regulated entity cybersecurity risk management costs discounted at seven percent. TSA uses each mode's annualized value in the break-even analysis to measure against the benefits of averting the costs from an attack to each surface mode.

[389] As previously discussed, TSA uses the full cost of the CRM program in this break-even analysis without adjusting for costs industry has incurred as a result of prior industry practices of TSA SDs.

Table 4-3: Cybersecurity Risk Management Costs Attributable to Each Surface Mode ($ Thousands)

Year	Freight Rail Costs	PTPR Costs	Pipeline Costs	Freight Rail Costs	PTPR Cost	Pipeline
	Undiscounted			Discounted at 7%		
	a = Table 3-25 + Column a Table 4-1	b = Table 3-50 + Column b, Table 4-1	c = (Column i, Table 3-80 - Column b, Table 3-80) + Column c, Table 4-1	d	e	f
1	$99,021.7	$120,639.1	$87,938.3	$92,543.6	$112,746.8	$82,185.3
2	$96,175.8	$120,972.3	$82,390.1	$84,003.7	$105,661.9	$71,962.7
3	$95,328.7	$121,849.6	$80,399.9	$77,816.6	$99,465.5	$65,630.3
4	$97,362.8	$124,065.0	$82,952.0	$74,277.6	$94,648.6	$63,283.7
5	$96,549.4	$124,998.9	$80,984.7	$68,838.4	$89,122.5	$57,741.0
6	$99,039.0	$127,476.5	$84,228.2	$65,993.9	$84,942.9	$56,124.8
7	$98,251.1	$128,470.0	$82,284.5	$61,185.8	$80,004.6	$51,242.6
8	$100,772.9	$131,014.1	$85,552.4	$58,650.7	$76,251.4	$49,792.3
9	$100,017.4	$132,070.2	$83,633.5	$54,402.8	$71,837.4	$45,491.1
10	$102,572.1	$134,683.5	$86,926.6	$52,142.5	$68,466.3	$44,189.1
Total	**$985,090.8**	**$1,266,239.1**	**$837,290.2**	**$689,855.6**	**$883,148.0**	**$587,642.8**
Annualized				**$98,219.9**	**$125,740.4**	**$83,667.1**

To evaluate CRM program break-even points, TSA presents a selection of potential consequence levels along with illustrative examples of the type of incident that could result in a similar level of damage or consequence for each mode of transportation.[390] TSA uses this approach due to the uncertain yet growing threat associated with cyber incidents.

Cyber-attacks are typically focused on denial of service or business disruption, data breach of internal information, and infrastructure/asset manipulation which in some cases have monetary implications. Each type of attack may result in different direct and indirect consequences including damage, loss of life, incident response, delay of services, and added inefficiencies

[390] The examples provided represent the type of security incidents that may occur but do not include all possible attacks or incidents nor suggest that the identified situations are the most likely or represent the highest vulnerability to a cybersecurity incident.

(e.g., having to ship products via alternative more expensive means).[391] Such attack impacts can be amplified or reduced based on specific circumstances of the event. For example, smaller versus larger/multiple targets, duration of disruption, as well as severity of outcomes (e.g., derailing trains in an open non-populated area versus a bridge, tunnel, or city center) impact the level of consequence.

4.3.2 Freight Railroad Scenarios

To break even, or for the benefits to justify the costs, the CRM program would need to prevent an average of approximately $98.22 million in aggregate freight rail consequence per year. This value is equal to the estimated freight rail annualized cost of the CRM program.[392] To help evaluate this loss avoidance, TSA calculates the level of risk reduction necessary for these annualized costs to break-even against events that result in $1 billion, $10 billion, and $20 billion in consequence.

The American Association of Railroads (AAR) estimates that a complete nationwide shutdown of freight rail transportation could cost more than $2 billion a day.[393] Based on this estimate, if just five percent of freight transport is affected for 5-10 days it could result in $500 million to $1 billion in impacts from the shutdown alone. This impact would increase to $5 billion (25 percent shutdown for 10 days), and $10 billion (50 percent shutdown for 10 days) with more severe

---

[391] Direct consequences capture economic losses that can be clearly linked to an incident without intermediate connections (e.g., the replacement cost of a train for an incident that causes a train derailment). Indirect consequences capture economic losses that are caused or augmented by an incident but a couple steps removed (e.g., the need to re-route trains due to an incident that causes a train derailment).

[392] TSA estimates the full CRM program annualized cost (discounted at 7 percent) over the 10 year period of analysis for freight rail is approximately $98,219,923; therefore, this is also the level of consequence that needs to be avoided for costs to equal "benefits."

[393] Association of American Railroads. (2022). The Economic Impact of a Railroad Shutdown. Retrieved September 28, 2023, (p. 2) from https://www.aar.org/wp-content/uploads/2022/09/AAR-Rail-Shutdown-Report-September-2022.pdf.

incidents increasing to $20 billion for a complete shutdown.

Although not the result of a cybersecurity incident, the 2023 derailment of a freight train transporting hazardous materials in East Palestine, Ohio provides an example of a potential $1 billion event if malicious cyber actors were able to gain access to a traffic control system and cause a similar type of incident.[394] A more recent settlement between Norfolk Southern and the Federal government has added $310 million to this total. The latest settlement between the U.S. Department of Justice and Norfolk Southern includes $15 million in penalties and a substantial additional sum to compensate EPA for expenses incurred in its cleanup efforts.[395] Principal costs include site clean-up (e.g., removing contaminated soil and tainted water), community support and compensation, and legal fees as well as other environmental impacts, railway traffic delays, and response/recovery costs not quantified.

An illustrative example of a larger cybersecurity incident involves widespread freight railroad systems failures resulting from Advanced Persistent Threat actor(s) on Class I and other major railroad carriers.[396] This threat includes a simultaneous cyber-attack on all Class I railroads impacting critical systems such as key connections to data networks (requiring railroads to revert to manual verification to maintain operations at a reduced capacity), access to remotely operated

---

[394] Isidore, C. (2023, July 27). East Palestine train derailment has now cost Norfolk Southern $1 billion. CNN. Retrieved September 28, 2023, from https://www.cnn.com/2023/07/27/investing/norfolk-southern-east-palestine-derailment-costs/index.html.

[395] Joselow, M. (2024, May 23). Norfolk Southern agrees to $310M settlement over Ohio train derailment. Washington Post. Retrieved June 20, 2024, from https://www.washingtonpost.com/climate-environment/2024/05/23/train-derailment-settlement-east-palestine/.

[396] Advanced persistent threat actor(s) is a well-resourced adversary engaged in sophisticated malicious cyber activity that is targeted and aimed at prolonged network/system intrusion. Objectives of such actor(s) could include espionage, data theft, and network/system disruption or destruction. "Advanced Persistent Threats and Nation-State Actors". CISA. https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats-and-nation-state-actors. Retrieved December 1, 2023.

signaling and switching (restricting train speeds and slowing operations), and internal communications and staffing systems disrupting railroads' ability to staff train operations. Such attacks may also be geographically targeted to proximity of key port facilities, DOD installations, and key system interchanges.

None of these events in and of themselves would result in complete stoppage of rail traffic across the Nation's rail network. However, these attacks, done concurrently, would likely result in delays that cascade across the network resulting in larger, longer, and more widespread impacts especially the longer they last. Traffic backups and delays would have downstream impact on most sectors of the Nation's economy. For example, extensive delays in vital commodities such as chlorine for water treatment plants and coal for electric power plants may result in the loss or reduction of critical services. Furthermore, the impact of these delays would grow as the duration of the incident increases as it would take time to work through the backlog of rail traffic once the system had been restored. A partial reopening and industry adjustments might mitigate some of these costs, but it is also possible that sustained disruption and delays will further create cascading effects throughout the economy.

Table 4-4 presents the amount of risk reduction that would be needed for the estimated costs of freight rail CRM program to break even for each of the three identified consequence levels ($1 billion, $10 billion, and $20 billion) as well as the number of years a cybersecurity incident would need to be prevented. For each of the three identified consequence levels, TSA calculates an annual risk-reduction value to the affected freight railway industry. Stated another way, the rule would need to reduce the likelihood of one or more successful cybersecurity incident of the specified magnitude by a certain percentage annually for the benefits to justify the estimated costs. These consequence amounts could be interpreted either as the expected value of

consequences from an attack of that size occurring with certainty (e.g. 100%), or of an even larger consequence event occurring with either less certainty or reduced impact (e.g. 50% chance, or partial impact, of a $20 billion even). For reporting purposes, TSA labels these as $10 billion-equivalent event. TSA also estimates the number of years the proposed rule would have to prevent such a cybersecurity incident to break even. For a $1 billion-equivalent event the required amount of annual risk reduction is approximately 0.098, or about 9.8 percent ($98.2 million ÷ $1 billion). For the same size $1 billion-equivalent event, the CRM program would need to prevent at least one or more incidents of this size approximately every 10.2 years ($1 billion ÷ $98.2 million). For a $10 billion-equivalent event, the CRM program would require a 0.98 percent reduction ($98.2 million ÷ $10 billion) or prevent at least one or more incidents of this size approximately every 101.8 years ($10 billion ÷ $98.2 million). A $20 billion-equivalent event requires a 0.49 percent reduction ($98.2 million ÷ $20 billion) or prevention of such an incident about every 204 years ($20 billion ÷ $98.2 million).

Table 4-4: Freight Rail Summary of Full CRM Program Break-Even Results

Breakeven Example	Annualized Cost of CRM Program (7% discount rate)	Consequence (Avoided Losses)-Equivalents	Required Risk Reduction	Required Frequency of Averted Cybersecurity Incidents
	a	b	c = a ÷ b	d = b ÷ a
$1 Billion Example	$98.22 million	$1 Billion	0.0982	One every 10.18 years
$10 Billion Example		$10 Billion	0.0098	One every 101.81 years
$20 Billion Example		$20 Billion	0.0049	One every 203.62 years

The level of required risk reduction is lower if the freight railroad costs from TSA's sensitivity analysis in Section 3.8 are used in the calculation. As presented in Table 4-5, risk reduction associated would be 6.6 percent or one about every 15 years for a $1 billion-equivalent event, 0.66 percent or one every 152 years for a $10 billion-equivalent event, and 0.33 percent or one about every 303 years for a $20 billion-equivalent event.

Additionally, with the proper incident response and critical cyber system procedures in place, even a successful attack which compromises one system might have a lower impact on an entity that is in compliance with the rule because of effective network segmentation. This would in aggregate likely lessen the consequence magnitude of a successful attack on the specific regulated entity and diminish cascading impacts.

Table 4-5: Freight Rail Summary of Sensitivity CRM Program Break-Even Results

Break-even Example	Annualized Cost of CRM Program (7% discount rate)	Consequence (Avoided Losses)-equivalent	Required Risk Reduction	Required Frequency of Averted Cybersecurity Incidents
	a	b	c = a ÷ b	d = b ÷ a
$1 Billion Example	$65.949 million	$1 Billion	0.0659	One every 15.16 years
$10 Billion Example		$10 Billion	0.0066	One every 151.63 years
$20 Billion Example		$20 Billion	0.0033	One every 303.27 years

4.3.3 Passenger Transit and Passenger Railroad (PTPR) Scenarios

To break even, or for the benefits to justify the costs, the CRM program would need to prevent an average of approximately $125.8 million in aggregate PTPR consequence per year. This value is equal to the estimated PTPR annualized cost of the CRM program.[397] To help evaluate this loss avoidance, TSA calculates the level of risk reduction necessary for the CRM program costs to break even against events that result in $1 billion-equivalent, $2 billion-equivalent and $4 billion-equivalent in consequence.

A cybersecurity incident that causes a signal to malfunction and results in the collision or derailment of a passenger train provides an illustrative example of a $1 billion-equivalent event. In this situation, lives are lost, people are injured, trains are destroyed or damaged, and

[397] TSA estimates the full CRM program annualized cost (discounted at 7 percent) over the 10-year period of analysis for PTPR is $125,740,410; therefore, this is also the level of consequence that needs to be avoided for costs to equal "benefits."

infrastructure may need repair.[398] For example, if an incident were to result in 50 fatalities and 200 injuries ranging in severity, the estimated consequence of fatalities based on the U.S. Department of Transportation (DOT) the valuation of statistical life (VSL) of $12.5 million is $625 million.[399] Assuming a range of injuries based on DOT's maximum abbreviated injury scale (MAIS) could add another $62.8 million.[400] Assuming one locomotive and five train cars require replacement plus $500,000 in track replacement adds another $17.7 million.[401] Factoring in additional response costs to address the cybersecurity incident and its physical repercussions as well as indirect costs related to portions of the track being shut down (causing delays) and potential fear induced impacts, the impact of such an incident may easily approach $1 billion or more especially if more trains are involved.

---

[398] A targeted attack on one or more passenger trains could result in a high number of fatalities and injuries. For example, a coordinated attack against two or three transit agencies could cause collisions or derailments, which could injure or kill dozens. Amtrak train 188's derailment in 2015 near Philadelphia, Pennsylvania injured 185 individuals and killed eight people (see National Transportation Safety Board 2016, retrieved August 27, 2024 from https://www.ntsb.gov/investigations/pages/DCA15MR010.aspx). Additionally, in 2013, a Metro North train derailed near Bronx, New York, injuring 61 and killing four (see National Transportation Safety Board 2014, retrieved August 27, 2024 from https://www.ntsb.gov/investigations/Pages/DCA14MR002.aspx). Finally, in June 2009, a collision on Washington Metropolitan Area Transit Authority (WMATA) metro rail near Fort Totten, Maryland injured approximately 80 and killed nine (see National Transportation Safety Board 2010, retrieved August 27, 2024 from https://www.ntsb.gov/investigations/Pages/DCA09MR007.aspx).

[399] U.S. Department of Transportation. (2021). Guidance on treatment of the economic value of a statistical life (VSL) in U.S. Department of Transportation analyses - 2021 update (p. 10, Table 2). 50 fatalities × $12.5 million VSL = $625 million. Retrieved October 12, 2023, from https://www.transportation.gov/sites/dot.gov/files/2021-03/DOT%20VSL%20Guidance%20-%202021%20Update.pdf

[400] Injuries on the MAIS scale are represented as a percentage of VSL with 0.3 percent ($37,200) for category 1 MAIS (minor), 4.7 percent ($582,800) for category 2 MAIS (moderate), 10.5 percent ($1,302,000) for category 3 MAIS (serious), 26.6 percent ($3,298,400) for category 4 MAIS (severe), and 59.3 percent ($7,355,200) for category 5 MAIS (critical). In this example, TSA estimates 147 passengers/crew injured at MAIS 1, 26 at MAIS 2, 23 at MAIS 3, 3 at MAIS 4, and 1 at MAIS 5. Applying the corresponding costs (147 x $37,200 + 26 x $582,800 + 23 x $1,302,000 + 1 x $7,355,200) results in $62,800,000.

[401] Train and car replacement = ($7,237,000.00 x 1 locomotive + $1,514,000.00 x 5 passenger cars) = $14,807,000.00. This is $17,246,006.19 in 2022 adjusted dollars using GDP deflation. Locomotive replacement, car replacement and rail replacement are based on Amtrak Passenger Train 501 Derailment. National Transportation Safety Board. (2019). Railroad Accident Report: Amtrak Passenger Train 501 Derailment DuPont, Washington December 18, 2017 (Report No. NTSB/RAR-19/01). Retrieved October 12, 2023, (See Table 2 and pp. 20-21) from https://www.ntsb.gov/investigations/AccidentReports/Reports/RAR1901.pdf.

A cybersecurity incident that causes the shutdown of one or more municipal rail systems provides an illustrative example of a $2 billion-equivalent event. The main impact driver of this type of event is the shutdown of municipal rail service that affects the ability and timeliness of passengers to get to their desired destinations. TSA uses DOT's Value of Time Travel Savings (VTTS) guidance to calculate the time impact of such delays. According to the DOT guidance, 95.4 percent of local surface travel is assumed to be personal travel (commuters are included in personal travel) and 4.6 percent is assumed to be business travel.[402] Furthermore, DOT uses 50 percent of the Census Bureau's median household income to approximate the lost value of time for personal travel and 100 percent to approximate median gross hourly compensation for business travel. Census's median household income in 2022 was $35.86 per hour.[403] This results in an estimated weighted average intercity surface travel delay cost of $18.62 per hour.[404]

Therefore, if malicious cybersecurity actors are able execute a coordinated attack and lock the central controls of one or more municipal rail systems resulting in the shutdown or delay of operations for an extended period of time; it could result in major impacts. Assuming an impact on a combined daily ridership of 8 million where on the first day of the incident trips are delayed for an average of 4 hours, as the population navigates the sudden closure, then delayed by an average of 1 hour for the remainder of the week, and an average of half an hour in the second

---

[402] U.S. Department of Transportation. (2014). Revised Departmental Guidance on Valuation of Travel Time in Economic Analysis. Retrieved September 28, 2023, from https://www.transportation.gov/sites/dot.gov/files/docs/USDOT%20VOT%20Guidance%202014.pdf. (see p. 12).

[403] U.S. Census Bureau. (2023). Median Household Income in the United States in 2022. Real median household income of $74,580 was divided by 2080 hours to calculate a median household income of $35.86. Retrieved October 3, 2023, from https://www.census.gov/library/publications/2023/demo/p60-279.html Please refer to Table A-1 and Figure 1 for more details.

[404] Average intercity surface travel delay cost = (95.4% personal travel × $35.86 median household hourly wage × 50%) + (4.6% business travel × $35.86 median household hourly wage × 100%) = $18.62 (rounded to the nearest hundredth).

week before service can return back to normal results in 145 million hours of delay.[405] TSA believes such residual delays, even weeks after the start of an incident, can stem from running train operations more slowly for a period of time and/or getting systems up and running again at full capacity. Using the average local surface travel delay cost of $18.62 per hour results in a delay in travel time cost of $2.0 billion.[406] TSA recognizes that many companies may allow for telework which would reduce these impacts to the extent workers could forgo commuting and work remotely.

A coordinated cybersecurity attack across multiple owner/operators with longer shutdown and more extensive delay periods could increase this impact to $4 billion. Again, assuming a combined ridership of 8 million and three weeks of impact, where trips are delayed for an average of four hours for the first day of the incident as the population navigates the sudden closure. The systems continue to be shut down for four additional days with trips delayed for an average of two hours as the population navigates the closure. The systems are then partially reopened or at a reduced capacity with delays persisting for an average of 1 hour for the first seven days as the systems reopen, and then by an average of half an hour in the for the following nine days before service can return to normal. This results in 188 million delay hours.[407] Using the average local surface travel delay cost of $18.62 per hour results in a delay in travel time cost

[405] Delay hours = (1 day × 4 hours + 7 days × 1 hour + 7 days × 0.5 hours) x 8,000,000 riders per day = 108,000,000. TSA assumes that even as some of the ridership switches modes as the delays persist, the delay hours would remain unchanged regardless of the type of alternative mode used due potentially slower means of transportation and/or similar delay impacts due to increased congestion.

[406] Value of Travel Delay = 108,000,000 delay hours × $18.62 average weighted wage = $2,010,800,000.

[407] Delay hours = (1 day × 4 hours + 4 days x 2 hours + 7 days × 1 hour + 9 days × 0.5 hours) x 8,000,000 riders per day = 188,000,000. TSA assumes that even as some of the ridership switches modes as the delays persist, the delay hours would remain unchanged regardless of the type of alternative mode used due potentially slower means of transportation and/or similar delay impacts due to increased congestion.

of $3.5 billion.[408] Factoring in additional response costs to address the cybersecurity incident and any physical repercussions as well as potential fear induced impacts, the impact of such an incident would likely approach $4 billion.

Table 4-6 presents the amount of risk reduction that would be needed for the PTPR CRM program to break even for each of the three identified consequence levels ($1 billion-equivalent, $2 billion-equivalent, and $4 billion-equivalent) as well as the number of years a cybersecurity incident would need to be prevented. For each of the three identified consequence levels, TSA calculates an annual risk-reduction value to an affected public transit entity. Stated another way, this proposed rule would need to reduce the likelihood of one or more successful cybersecurity incident of the specified magnitude by a certain percentage annually for the benefits to justify the estimated costs.[409] TSA also estimates the number of years the proposed rule would have to prevent a cybersecurity incident to break even. For a $1 billion-equivalent event the required amount of annual risk reduction is approximately 0.126, or about 12.6 percent ($125.7 million ÷ $1 billion) For a $1 billion-equivalent event, the CRM program would need to prevent at least one or more incidents of this size approximately every 8 years ($1 billion ÷ $125.7 million). TSA

---

[408] Value of Time Travel Savings = 188,000,000 delay hours × $18.62 average weighted wage = $3.5 billion

[409] While various cyber attacks of differing magnitudes occur each year, TSA does not have comprehensive data on the specific number and magnitude of such attacks in order to estimate an attack frequency. In addition, the rule aims to prevent and/or limit the impact of potential larger events that do not have historical equivalents. Nonetheless, examples of past attacks include ransomware attacks on the San Francisco Municipal Transportation Agency (SFMTA) in 2016 and Southeastern Pennsylvania Transportation Authority and Fort Worth's Trinity Metro transit agency in 2020 (retrieved August 27, 2024 from https://www.phillyvoice.com/septa-cyberattack-malware-august-2020-emails-security-philadelphia/). As mentioned above, cyber attacks can have physical consequences, such as collisions or derailments, resulting in damages similar to those of recent non-cyber-attack incidents, such as the 2013 Metro-North and 2015 Amtrak train 188 derailments and 2009 WMATA train collision (retrieved August 27, 2024 from https://www.ntsb.gov/investigations/). However, these examples should not be considered exhaustive of the wide-ranging scale, scope, or frequency of potential cyber attacks. TSA also refers back to the March 2023 CISA advisory, cited and discussed in Section 1.3, which notes that vulnerabilities can allow attackers to "take control of affected systems, manipulate and modify settings, escalate privileges, bypass security controls, steal data, and crash systems."

performs a similar calculation for a $2 billion-equivalent event which requires a 6.3 percent reduction ($125.7 million ÷ $2 billion) or prevention of such an incident about every 16 years ($2 billion ÷ $125.7 million). A $4 billion-equivalent event requires a requires a 3.1 percent reduction ($125.7 million ÷ $4 billion) or prevention of such an incident about every 32 years ($4 billion ÷ $125.78 million).

Table 4-6: PTPR Summary of Full CRM Program Break-Even Results

Break-Even Example	Annualized Cost of CRM Program (7% discount rate)	Consequence (Avoided Losses) equivalent	Required Risk Reduction	Required Frequency of Averted Cybersecurity Incident
	a	b	c = a ÷ b	d = b ÷ a
$1 Billion Example	$125.74 million	$1 billion	0.1257	One every 7.95 years
$2 Billion Example		$2 billion	0.0629	One every 15.91 years
$4 Billion Example		$4 billion	0.0314	One every 31.81 years

The level of required risk reduction is lower if PTPR railroad costs from TSA's sensitivity analysis in Section 3.8 are used in the calculation. As presented in Table 4-7, risk reduction associated would be 7.8 percent or one about every 13 years for a $1 billion-equivalent event, 3.9 percent or one about every 26 years for a $2 billion-equivalent event, and 1.9 percent or one about every 51 years for a $4 billion-equivalent event.

Table 4-7: PTPR Rail Summary of Sensitivity CRM Program Break-Even Results

Break-Even Example	Annualized Cost of CRM Program (7% discount rate)	Consequence (Avoided Losses) equivalent	Required Risk Reduction	Required Frequency of Averted Cybersecurity Incident
	a	b	c = a ÷ b	d = b ÷ a
$1 Billion Example	$78.063 million	$1 billion	0.0781	One every 12.81 years
$2 Billion Example		$2 billion	0.0390	One every 25.62 years
$4 Billion Example		$4 billion	0.0195	One every 51.24 years

4.3.4 Pipeline Scenarios

To break even, or for the benefits to justify the costs, the CRM program would need to prevent an average of approximately $83.7 million in aggregate pipeline consequence per year. This

value is equal to the estimated pipeline annualized cost of the CRM program.[410] To help evaluate this lost avoidance, TSA calculates the level of risk reduction necessary for the CRM program to break even against events that result in $2 billion-equivalent, $10 billion-equivalent, and $20 billion-equivalent in consequence.

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 as the disruption extends in length of time.[411] For instance, a pipeline disruption affecting gasoline distribution lasting a few days would have smaller impacts than a disruption lasting two weeks as reserves are used up, panic grows, and rationing may need to be implemented. Any disruption, or even potential disruption, can affect the price for gasoline, diesel or natural gas, for example when potential hurricanes cause evacuation and shut down of off-shore platforms in the Gulf Coast.[412] Negative impacts could be extended further as pipelines support critical utilities such as electricity generation. A 2007 paper discussing business interruption impacts resulting from electric power disruption estimates the cost of a two-week electricity outage to a major metropolitan county (approximately 10,000 sq. miles and 9 million people) as between $0.289 billion to $2.2 billion per day, depending on the

---

[410] TSA estimates the full CRM program annualized cost (discounted at 7 percent) over the 10-year period of analysis for pipeline, including TSA costs proportionally applied to all modes is $83,690,592; therefore, this is also the level of consequence that needs to be avoided for costs to equal "benefits."

[411] According to PHMSA, the Nation's more than 2.6 million miles of pipelines safely deliver trillions of cubic feet of natural gas and hundreds of billions of ton/miles of liquid petroleum products each year. They are essential: the volumes of energy products they move are well beyond the capacity of other forms of transportation. It would take a constant line of tanker trucks, about 750 per day, loading up and moving out every two minutes, 24 hours a day, seven days a week, to move the volume of even a modest pipeline. The railroad-equivalent of this single pipeline would be a train of 225, 28,000-gallon tank cars. https://www.phmsa.dot.gov/faqs/general-pipeline-faqs#QA_5

[412] According to the U.S. Energy Information Administration, in 2022 an average of about 370 million gallons of finished motor gasoline were consumed per day. Frequently Asked Questions (FAQs) - U.S. Energy Information Administration (EIA). An overall price disruption of $1 for 5 days would add $1.85 billion in inefficiency.

level of resilience and preparedness of the community.[413]

TSA estimates the value of pipeline materials transported ranges from approximately $2 billion[414] to $2.9 billion[415] per day. Assuming a 5 to 15 percent delay cost against this value results in a daily impact range of $0.1 billion to $0.435 billion per day.[416] Based on these estimates, a 5 to 20-day disruption equates to between $0.5 billion to $8.7 billion in delay costs; not accounting for other societal impacts.

Other pipeline related impacts could occur specifically as part of a utility disruption. For instance, a cyber attack may disable safety controls regarding the allowable pressure of product flow in a pipeline. While not a cybersecurity incident itself, a 2018 natural gas pipeline incident in Merrimack Valley, Massachusetts provides an example of the type and scale of consequence

---

[413] See Rose, A., S. Liao and G. Oladosu, "Business Interruption Impacts of a Terrorist Attack on the Electric Power System of Los Angeles: Customer Resilience to a Total Blackout," Risk Analysis, Vol. 27, No. 3, 2007. Converted to 2022 dollars per day, original estimates $2.8 billion to $20.5 billion (2005 dollars for full two-week outage, see p. 528).

[414] TSA gathers the volume of crude oil and refined petroleum products shipped via pipeline from Bureau of Transportation Statistics (BTS) 2021 annual values from BTS, Table 1-61. "Crude Oil and Petroleum Products Transported in the United States by Mode." BTS. April 2022. https://www.bts.gov/content/crude-oil-and-petroleum-products-transported-united-states-mode. BTS reported 1,164 million barrels of crude oil and 2,263 million barrels for refined petroleum products was shipped via pipeline in 2021. Energy Information Association (EIA), "Natural Gas Annual 2022," https://www.eia.gov/naturalgas/annual/ reports that the U.S. produced 36.4 trillion cubic feet of natural gas in 2022. EIA also reports the price of natural gas averaged $6.67 per 1,000 cubic feet in 2022. TSA multiplies the price of crude oil's annual average from 2022 ($94.91/barrel) by the volume of crude oil shipped and adds to it the product of natural gas shipped and its annual average price from 2022. TSA calculates a weighted average price of refined products of $4.14/gal or $173.89/barrel. TSA multiplies the volume of refined petroleum products shipped by the weighted average price and adds to the other components. The total value of products shipped via pipeline in 2022 is calculated as $746,934 million. This amount is $2,046 million per day ($746,934 million ÷ 365).

[415] Freight Analysis Framework (FAF) database. "Freight Analysis Framework" Oak Ridge National Laboratory. Accessed on October 13, 2023. https://faf.ornl.gov/faf5/dtt_total.aspx. The value of products shipped via pipeline in 2022. Identifies an annual amount of $1.057 trillion which TSA divides by 365 to yield a daily value of approximately $2.895 billion per day.

[416] TSA assumes an interest rate between 5 and 15 percent to account for delay costs, but the value could be higher. TSA relates the cost of delay with the cost of inventory. Disruptions in business operations mean that firms may have to hold higher levels of inventory due to missed/delayed shipments which would be financed through capital at a marginal cost of the interest rate; or in other words, the interest on the value of the delayed shipments.

that may occur related to a pipeline incident with utility disruption.[417] A series of structure fires and explosions occurred after a high-pressure gas was released into a low-pressure distribution system resulting in one death and 22 injuries. Additional impacts include numerous structures being damaged including five homes which were completely destroyed, over 10,000 customers losing gas service for a period of time, and 50,000 residents in the affected area being evacuated due to safety concerns. News reports indicate associated costs of over $1 billion.[418] The Pipeline Hazardous Materials and Safety Administration (PHMSA) reported the value of all damages as over $1.7 billion.[419] A cyber incident could result in similar consequences through an exploited vulnerability that allows for the disruption of the distribution system (e.g., by disabling or altering safety controls) resulting in damages to equipment and possible explosion. If such events happened on a larger scale, the impact would only increase.

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. However, given the nature of the pipeline industry and anticipated inventory stores, such impacts wouldn't likely rise to this level of impact until after about 5 days. Table 4-8 shows the potential impact of varying percentage reductions in system-wide throughput and number of days impacted. TSA notes there is a distinction between the number of days over which an incident

---

[417] "Pipeline Accident Report. NTSB/PAR-19/02 PB2019-101365." National Transportation Safety Board. September 14, 2019. Accessed September 28, 2023. https://www.ntsb.gov/investigations/AccidentReports/Reports/PAR1902.pdf.

[418] The Boston Herald, "Columbia Gas parent company says cost for Merrimack Valley gas disaster could hit $1B," May 1, 2019. Retrieved Oct. 14 from https://www.bostonherald.com/2019/05/01/nisource-ups-cost-estimates-for-merrimack-valley-gas-disaster/. The Haverhill Gazette, "The Week in Review," March 7, 2019. Retrieved Oct. 14, 2023 from https://www.hgazette.com/news/local_news/the-week-in-review/article_29f8c315-50b8-55d1-90cc-79776af36b14.html.

[419] PHMSA, Pipeline Incident 20 Year Trends, Significant Incident Listing (as of 10/13/2023). Report ID: 20180092. Pipeline Incident 20 Year Trends | PHMSA (dot.gov). Reports total cost current year dollars as $1,793,700,872.

stretches and the number of days of shutdown impact at the aforementioned $1 to $2 billion-equivalent; and that the number of days impacted begin following the initial 5 days when inventory stores can be relied upon.[420] The values in the table below represent the percentage of pipeline volume impacted multiplied by $1.5 billion-equivalent disruption impact per day (midpoint between $1 and $2 billion) and the number of days impacted. For instance, if 30 percent of the system were shut down for 5 days, the estimated impact equates to $2.25 billion (30 percent × $1.5 billion per day × 5 days).

Table 4-8: Economic Impact Projection (in Billions) of Pipeline Shutdown by Number of Days Impacted and Percent of Pipeline Volume Impacted

Percent of Pipeline Volume Impacted	Number of Days Impacted			
	5	10	15	20
20%	$1.50	$3.00	$4.50	$6.00
30%	$2.25	$4.50	$6.75	$9.00
40%	$3.00	$6.00	$9.00	$12.00
50%	$3.75	$7.50	$11.25	$15.00
60%	$4.50	$9.00	$13.50	$18.00
70%	$5.25	$10.50	$15.75	$21.00
80%	$6.00	$12.00	$18.00	$24.00

For its break-even analysis, TSA uses a 15-day shutdown impacting 50 percent of pipeline volume at an estimated impact of $1-2 billion a day (starting after day 5 and therefore 10-day impact) equates to a $5 - $10 billion event and a 20-day shutdown at 75 percent of pipeline volume equates to a $11.25 - $22.5 billion event. Table 4-9 presents the amount of risk reduction that would be needed for the estimated costs of the pipeline CRM program to break even for each of the three identified consequence levels ($2 billion-equivalent, $10 billion-equivalent, and

[420] Many fuel distributors keep at least 5 days' inventory on hand for emergencies and delays; hence reduced impacts in the initial days of a disruption. For example, as discussed in Section 1.1, when a major pipeline operator was the victim of a cyber attack in May 2021, the incident was less impactful than it could have been because it only lasted 5 days but could have had a much greater impact if the incident lasted longer. Therefore, the number of days of shutdown would increase the number of impacted days from the table plus 5 days.

$20 billion-equivalent) as well as the number of years a cybersecurity incident would need to be prevented.

For each of the three identified consequence levels, TSA calculates an annual risk-reduction value to an affected pipeline company. Stated another way, this proposed rule would need to reduce the likelihood of one or more successful cybersecurity incident of the specified magnitude by a certain percentage annually for the benefits to justify the estimated costs. TSA also estimates the number of years the proposed rule would have to prevent a cybersecurity incident to breakeven. For a $1 billion-equivalent event the required amount of annual risk reduction is approximately 0.042, or about 4.2 percent ($83.7 million ÷ $2 billion). For the same size $2 billion-equivalent event, the CRM program would need to prevent at least one or more incidents of this size approximately every 24 years ($2 billion ÷ $83.7 million). TSA performs a similar calculation for a $10 billion-equivalent event which requires an 0.84 percent reduction ($83.7 million ÷ $10 billion) or prevention of such an incident about every 119 years ($10 billion ÷ $83.7 million). A $20 billion-equivalent event requires a requires a 0.42 percent reduction ($83.7 million ÷ $20 billion) or prevention of such an incident about every 239 years ($20 billion ÷ $83.7 million).

Table 4-9: Pipeline Summary of Full CRM Program Break-Even Results

Break-Even Example	Annualized Cost of CRM Program (7% discount rate)	Consequence (Avoided Losses) equivalent	Required Risk Reduction	Required Frequency of Averted Cybersecurity Incident
	a	b	c = a ÷ b	d = b ÷ a
$2 Billion Example	$83.667 million	$2 Billion	0.0418	One every 23.90 years
$10 Billion Example		$10 Billion	0.0084	One every 119.52 years
$20 Billion Example		$20 Billion	0.0042	One every 239.04 years

The level of required risk reduction is lower if pipeline costs from TSA's sensitivity analysis in Section 3.8 are used in the calculation. As presented in Table 4-10, risk reduction associated

would be 3.2 percent or one about every 32 years for a $2 billion-equivalent event, 0.63 percent or one about every 158 years for a $10 billion-equivalent event, and 0.32 percent or one about every 316 years for a $20 billion-equivalent event.

Table 4-10: Pipeline Summary of Sensitivity CRM Program Break-Even Results

Break-Even Example	Annualized Cost of CRM Program (7% discount rate)	Consequence (Avoided Losses) equivalent	Required Risk Reduction	Required Frequency of Averted Cybersecurity Incident
	a	b	c = a ÷ b	d = b ÷ a
$2 Billion Example	$63.222 million	$2 Billion	0.0316	One every 31.63 years
$10 Billion Example		$10 Billion	0.0063	One every 158.17 years
$20 Billion Example		$20 Billion	0.0032	One every 316.35 years

4.4 Benefit Summary

TSA expects this rulemaking would provide numerous benefits to the security of freight railroad, passenger railroad, and pipelines. Physical security requirements for OTRB and pipelines provide potential benefits through increased awareness and tracking of security threats across the industry through incident reporting in addition to improved communication through designated pipeline security coordinators. However, TSA believes most of the rule's benefits are derived from the development of a CRM program which could reduce the risk and impact of a cybersecurity incident. Requirements of the proposed rule would help enhance the security of the regulated population which could reduce the chance of negative consequences and service interruptions for surface modes being regulated. Requiring owner/operators to proactively develop cybersecurity programs to protect critical systems, plan how they would respond to attacks, and regularly assess the performance of their programs would help owner/operators identify, protect, detect, respond to, and recover from a wide range of cybersecurity incidents.

As noted in the break-even discussion, 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.

The requirements of this NPRM provide a blueprint for improving defenses against cybersecurity incidents. Industry experience indicates that having a defense-in-depth cybersecurity approach helps defend against breaches of operational systems and compromises of customer information.[421] TSA anticipates the proposed rule's requirements, such as enhancing system security, maintaining backups, monitoring systems, and developing a response plan, will strengthen cybersecurity defenses over the long term. A commitment to patching management, system segmentation, and adding firewalls might limit the resources potential malicious actors would be able to access during an intrusion. The presence of backups allows for system restoration, data recovery, maintaining compliance and unhindered system operations. Continuous monitoring of the network will help to detect and respond to potential threats and limit system degradation. Having a response plan in place in case of a successful attack or cybersecurity incident may reduce its impact.

[421] Well-designed security systems have been credited for limiting damages in recent cyber incident cases: ABC7 New York. (2021, June 2). Hackers breached several of MTA's computer systems in April. Retrieved September 28, 2023, from https://abc7ny.com/mta-hack-computer-nyc-new-york-city/10734358/.

5 ANALYSIS OF ALTERNATIVES

Under the Office of Management and Budget (OMB) Circular A-4, the Transportation Security Administration (TSA) has to consider regulatory alternatives to the requirements in the proposed rule. Throughout the process of developing the proposed rule, TSA engaged in discussions regarding the elements that became the basis for the proposed rule's requirements. TSA analyzed alternatives to the proposed rule ("preferred alternative") in these discussions. In this section, TSA describes and analyzes three regulatory alternatives to the proposed rule.

- The first alternative (Alternative 1) represents a reduction in the scope of requirements, which would only include the identification of responsible persons for owner/operators, identification of critical cyber security systems, reporting of cybersecurity incidents, and the creation of a CIRP for each owner/operator.

- The second alternative (Alternative 2) represents different applicability standards that result in a smaller set of owner/operators impacted for each industry.

- The third alternative (Alternative 3) adds regulatory requirements to 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 criminal history records check for all cybersecurity coordinators and accountable executives in all industries.

TSA uses the methodology in Section 3 of this RIA to estimate the costs for all alternatives presented in this section. The differences observed in these alternatives result from changes in the requirements or affected population and not from the methodology used to estimate the costs. The potential benefits to security would vary among the alternatives depending on the changes in

the requirements or affected population. None of the previously discussed alternatives represent a statutory minimum as cybersecurity is a relatively new and evolving topic with limited explicit statutory language prescribing action. However, TSA's authorities do reference cybersecurity and there are statutes that stipulate security requirements which generally relate to or include the protection of IT and OT systems. Nonetheless, such requirements only encompass aspects of cybersecurity and thus make identifying a minimum statutory requirement difficult.

5.1 Alternative 1: Reduced Scope of Requirements

This alternative represents a reduction in the scope of requirements presented in the preferred alternative. It would require the identification of responsible persons for an owner/operator's CRM program, designation of a cybersecurity coordinator, identification of critical cybersecurity systems, the reporting of incidents to CISA/TSA, and the submission of an incident response plan. It includes some of the provisions in TSA's current Security Directives but does not require owner/operators to meet specific cybersecurity performance measures to protect against ransomware incidents and other known threats to IT and OT systems nor to conduct a cybersecurity evaluation nor assessment. Specific requirements, along with the cost to determine inclusion and costs for overall rule familiarization, include the following:

- Governance of the CRM Program (Sections 1580.309, 1582.209, and 1586.209 of proposed rule);
- Cybersecurity Coordinator (Sections 1580.311, 1582.211, and 1586.211 of the proposed rule);
- Identification of Critical Cybersecurity Systems (Sections 1580.313, 1582.213, and 1586.213 of the proposed rule);

- Reporting Cybersecurity Incidents (Sections 1580.325, 1582.225, and 1586.225 of the proposed rule); and

- Cybersecurity Incident Response Plan (Section 1580.327, 1582.227, and 1586.227 of the proposed rule).

5.1.1 Cost Impacts of Alternative 1 on Freight Rail Entities

This alternative would reduce the cost impact on freight rail entities relative to the preferred alternative. Table 5-1 lists the provisions included in the proposed rule and indicates which are incorporated into Alternative 1 using inputs from Table 3-25.

Table 5-1: Alternative 1 Provision Inclusion for Freight Rail

CFR Section	Proposed Rule Provision	Included in Alternative 1
1580.301	Scope and applicability	Yes
1580.303	Form, content, and availability of Cybersecurity Risk Management program.	No
1580.305	Cybersecurity evaluation	No
1580.307	Cybersecurity Operational Implementation Plan	No
1580.309	Governance of the CRM program	Yes
1580.311	Cybersecurity Coordinator	Yes
1580.313	Identification of Critical Cyber Systems	Yes
1580.315	Supply chain risk management	No
1580.317	Protection of Critical Cyber Systems	No
1580.319	Cybersecurity training and knowledge	No
1580.321	Detection of cybersecurity incidents	No
1580.323	Capabilities to respond to a cybersecurity incident	No
1580.325	Reporting cybersecurity incidents	Yes
1580.327	Cybersecurity incident response plan	Yes
1580.329	Cybersecurity Assessment Plan	No
1580.331	Documentation to establish compliance	No

For those requirements which remain part of the proposed rule under this alternative, the discounted cost impacts for freight rail entities would be equivalent to the discounted cost under the preferred alternative as shown in Table 5-2. A full discussion of the inputs and formula methodology for provision costs can be found in Section 3.1 with the derived summary table available in Table 3-25.

Table 5-2: Total Costs for Alternative 1 Requirements - Freight Rail ($ Thousands)

Year	Familiarization Costs	Designate Accountable Executive	Designate Cyber-security Coordinator and Alternate	Report Cyber-security Incidents to CISA	Identification of Critical Cyber Systems	Cyber-security Incident Response Plan (CIRP)	Record-keeping & Compliance	Total Costs h = ∑ a,b,c,d,e,f,g		
	a	b	c	d	e	f	g	Undiscounted	Discounted at 3%	Discounted at 7%
1	$242.2	$28.3	$37.6	$1.0	$1,129.2	$1,963.1	$276.4	$3,677.8	$3,570.7	$3,437.2
2	$2.0	$1.4	$1.8	$1.0	$291.1	$1,421.7	$278.6	$1,997.6	$1,939.4	$1,866.9
3	$2.0	$1.4	$1.8	$1.0	$293.3	$1,432.7	$280.8	$2,013.0	$1,954.3	$1,881.3
4	$2.0	$1.4	$1.8	$1.0	$295.7	$1,444.0	$283.0	$2,028.8	$1,969.7	$1,896.1
5	$2.0	$1.4	$1.9	$1.0	$298.1	$1,455.4	$285.2	$2,045.0	$1,985.4	$1,911.2
6	$2.0	$1.4	$1.9	$1.0	$300.4	$1,466.8	$287.4	$2,060.9	$2,000.9	$1,926.1
7	$2.0	$1.4	$1.9	$1.0	$302.6	$1,478.1	$289.7	$2,076.8	$2,016.3	$1,941.0
8	$2.1	$1.4	$1.9	$1.1	$305.1	$1,489.8	$291.9	$2,093.2	$2,032.3	$1,956.3
9	$2.1	$1.4	$1.9	$1.1	$307.4	$1,501.3	$294.2	$2,109.4	$2,048.0	$1,971.4
10	$2.1	$1.4	$1.9	$1.1	$309.9	$1,513.2	$296.5	$2,126.1	$2,064.2	$1,987.0
Total	**$260.3**	**$40.9**	**$54.4**	**$10.3**	**$3,832.8**	**$15,166.2**	**$2,863.6**	**$22,228.6**	**$21,581.2**	**$20,774.4**
Annualized									**$2,158.1**	**$2,077.4**

Note: Totals may not add due to rounding.

5.1.2 Cost Impacts of Alternative 1 on Passenger Transit and Passenger Rail Entities

This alternative would reduce the cost impact on PTPR entities relative to the preferred alternative. Table 5-3 lists the provisions included in the proposed rule and indicates which are incorporated into Alternative 1 using inputs from Table 3-50.

Table 5-3: Alternative 1 Provision Inclusion for PTPR

CFR Section	Proposed Rule Provision	Included in Alternative 1
1582.201	Scope and applicability	Yes
1582.203	Form, content, and availability of Cybersecurity Risk Management program.	No
1582.205	Cybersecurity evaluation	No
1582.207	Cybersecurity Operational Implementation Plan	No
1582.209	Governance of the CRM program	Yes
1582.211	Cybersecurity Coordinator	Yes
1582.213	Identification of Critical Cyber Systems	Yes
1582.215	Supply chain risk management	No
1582.217	Protection of Critical Cyber Systems	No
1582.219	Cybersecurity training and knowledge	No
1582.221	Detection of cybersecurity incidents	No
1582.223	Capabilities to respond to a cybersecurity incident	No
1582.225	Reporting cybersecurity incidents	Yes
1582.227	Cybersecurity incident response plan	Yes
1582.229	Cybersecurity Assessment Plan	No
1582.231	Documentation to establish compliance	No

For those requirements which remain part of the proposed rule under this alternative, the discounted cost impacts for PTPR entities would be equivalent to the discounted cost under the preferred alternative as shown in Table 5-4. A full discussion of the inputs and formula methodology for provision costs can be found in Section 3.2 with the derived summary table available in Table 3-50.

Table 5-4: Total Costs for Alternative 1 Requirements - PTPR ($ Thousands)

Year	Familiarization Costs	Designate Accountable Executive	Designate Cybersecurity Coordinator and Alternate	Report Cyber-security Incidents to CISA	Identification of Critical Cyber Systems	Cybersecurity Incident Response Plan (CIRP)	Recordkeeping & Compliance	Total Costs h = ∑ a,b,c,d,e,f,g		
	a	b	c	d	e	f	g	Undiscounted	Discounted at 3%	Discounted at 7%
1	$54.5	$8.5	$12.1	$1.3	$460.1	$871.4	$84.2	$1,492.3	$1,448.8	$1,394.6
2	$1.2	$1.3	$1.9	$1.3	$125.1	$674.6	$86.1	$891.4	$865.4	$833.1
3	$1.2	$1.3	$1.9	$1.3	$127.9	$689.5	$88.0	$911.2	$884.7	$851.6
4	$1.2	$1.4	$2.0	$1.3	$130.6	$704.4	$89.9	$930.8	$903.7	$869.9
5	$1.3	$1.4	$2.0	$1.4	$133.6	$720.0	$91.9	$951.5	$923.8	$889.2
6	$1.3	$1.4	$2.0	$1.4	$136.4	$735.7	$93.9	$972.2	$943.9	$908.6
7	$1.3	$1.5	$2.1	$1.4	$139.4	$751.8	$95.9	$993.5	$964.6	$928.5
8	$1.4	$1.5	$2.1	$1.5	$142.5	$768.3	$98.0	$1,015.3	$985.7	$948.9
9	$1.4	$1.5	$2.2	$1.5	$145.5	$785.0	$100.2	$1,037.3	$1,007.1	$969.5
10	$1.4	$1.6	$2.2	$1.5	$148.8	$802.3	$102.4	$1,060.3	$1,029.4	$990.9
Total	**$66.3**	**$21.5**	**$30.6**	**$14.0**	**$1,689.9**	**$7,503.1**	**$930.5**	**$10,255.8**	**$9,957.1**	**$9,584.9**
Annualized									**$995.7**	**$958.5**

Note: Totals may not add due to rounding.

5.1.3 Cost Impacts of Alternative 1 on Over the Road Bus Entities

This alternative would not change the cost impact on OTRB entities relative to the preferred alternative. While this alternative would have fewer requirements, the entirety of the Alternative 1 requirements are those that are already not applicable to OTRB. OTRB entities are only subject to the reporting of cybersecurity incidents which are not affected by this alternative. Therefore, the cost impact of the alternative relative to the preferred alternative is zero.

5.1.4 Cost Impacts of Alternative 1 on Pipeline Entities

This alternative would reduce the cost impact on pipeline entities relative to the preferred alternative. Table 5-5 lists the provisions included in the proposed rule and indicates which are incorporated into Alternative 1 using inputs from Table 3-80.

Table 5-5: Alternative 1 Provision Inclusion for Pipelines

CFR Section	Proposed Rule Provision	Included in Alternative 1
1586.201	Scope and applicability	Yes
1586.103	Physical security coordinator	No
1586.105	Reporting security incidents	No
1586.203	Form, content, and availability of Cybersecurity Risk Management program.	No
1586.205	Cybersecurity evaluation	No
1586.207	Cybersecurity Operational Implementation Plan	No
1586.209	Governance of the CRM program	Yes
1586.211	Cybersecurity Coordinator	Yes
1586.213	Identification of Critical Cyber Systems	Yes
1586.215	Supply chain risk management	No
1586.217	Protection of Critical Cyber Systems	No
1586.219	Cybersecurity training and knowledge	No
1586.221	Detection of cybersecurity incidents	No
1586.223	Capabilities to respond to a cybersecurity incident	No
1586.225	Reporting cybersecurity incidents	Yes
1586.227	Cybersecurity incident response plan	Yes
1586.229	Cybersecurity Assessment Plan	No
1586.231	Documentation to establish compliance	No

For those requirements which remain part of the proposed rule under this alternative, the discounted cost impact for pipeline entities would be equivalent to the discounted cost under the preferred alternative as shown in Table 5-6. A full discussion of the inputs and formula methodology for provision costs can be found in Section 3.4.10 with the derived summary table

available in Table 3-80.

Table 5-6: Total Costs for Alternative 1 Requirements - Pipelines ($ Thousands)

Year	Familiarization Costs	Designate Accountable Executive	Designate Cybersecurity Coordinator and Alternate	Report Cyber-security Incidents to CISA	Identification of Critical Cyber Systems	Cybersecurity Incident Response Plan (CIRP)	Record-keeping & Compliance	Total Costs h = ∑ a,b,c,d,e,f,g		
	a	b	c	d	e	f	g	Un-discounted	Discounted at 3%	Discounted at 7%
1	$911.6	$78.0	$91.6	$37.8	$1,703.7	$6,886.5	$644.6	$10,353.8	$10,052.3	$9,676.5
2	$0.0	$10.7	$12.5	$37.8	$425.9	$6,071.7	$644.6	$7,203.2	$6,993.4	$6,732.0
3	$0.0	$10.7	$12.5	$37.8	$425.9	$6,071.7	$644.6	$7,203.2	$6,993.4	$6,732.0
4	$0.0	$10.7	$12.5	$37.8	$425.9	$6,071.7	$644.6	$7,203.2	$6,993.4	$6,732.0
5	$0.0	$10.7	$12.5	$37.8	$425.9	$6,071.7	$644.6	$7,203.2	$6,993.4	$6,732.0
6	$0.0	$10.7	$12.5	$37.8	$425.9	$6,071.7	$644.6	$7,203.2	$6,993.4	$6,732.0
7	$0.0	$10.7	$12.5	$37.8	$425.9	$6,071.7	$644.6	$7,203.2	$6,993.4	$6,732.0
8	$0.0	$10.7	$12.5	$37.8	$425.9	$6,071.7	$644.6	$7,203.2	$6,993.4	$6,732.0
9	$0.0	$10.7	$12.5	$37.8	$425.9	$6,071.7	$644.6	$7,203.2	$6,993.4	$6,732.0
10	$0.0	$10.7	$12.5	$37.8	$425.9	$6,071.7	$644.6	$7,203.2	$6,993.4	$6,732.0
Total	**$911.6**	**$174.0**	**$204.3**	**$378.4**	**$5,536.9**	**$61,531.4**	**$6,446.0**	**$75,182.6**	**$72,992.8**	**$70,264.1**
Annualized									**$7,299.3**	**$7,026.4**

Note: Totals may not add due to rounding.

5.1.5 Cost Impacts of Alternative 1 on TSA

This alternative would reduce the cost impact on TSA relative to the preferred alternative. Table 5-7 lists the provisions included in the proposed rule and indicates which are incorporated into Alternative 1 using inputs from Table 3-25, Table 3-50, and Table 3-80.

Table 5-7: Alternative 1 Provision Inclusion for TSA

CFR Section	Proposed Rule Provision	Included in Alternative 1
1580.301, 1582.201, 1584.101, and 1586.201	Scope and applicability	Yes
1586.105	Reporting security incidents	No
1580.303, 1582.203 and 1586.203	Form, content, and availability of Cybersecurity Risk Management program.	No
1580.305, 1582.205 and 1586.205	Cybersecurity evaluation	No
1580.307, 1582.207 and 1586.207	Cybersecurity Operational Implementation Plan	No
1580.309, 1582.209 and 1586.209	Governance of the CRM program	Yes
1580.311, 1582.211, and 1586.211	Cybersecurity Coordinator	Yes
1580.313, 1582.213, and 1586.213	Identification of Critical Cyber Systems	Yes
1580.315, 1582.215, and 1586.215	Supply chain risk management	No
1580.317, 1582.217, and 1586.217	Protection of Critical Cyber Systems	No
1580.319, 1582.219 and 1586.219	Cybersecurity training and knowledge	No
1580.321, 1582.221, and 1586.221	Detection of cybersecurity incidents	No
1580.323, 1582.223, and 1586.223	Capabilities to respond to a cybersecurity incident	No
1580.325, 1582.225, 1584.107, and 1586.225	Reporting cybersecurity incidents	Yes
1580.327, 1582.227, and 1586.227	Cybersecurity incident response plan	Yes
1580.329, 1582.229, and 1586.229	Cybersecurity Assessment Plan	No
1580.331, 1582.231, and 1586.231	Documentation to establish compliance	No

For those requirements which remain part of the proposed rule under this alternative, the discounted cost impacts for TSA would be equivalent to the discounted cost under the preferred alternative as shown in Table 5-8. A full discussion of the inputs and formula methodology for provision costs can be found in Section 3.5.6 with the derived summary table available in Table 3-92.

Table 5-8: Total Costs for Alternative 1 Requirements - TSA ($ Thousands)

Year	Process Accountable Executive Information	Process Cybersecurity Coordinator Information	Training TSI's to Inspect New Programs	Process Cybersecurity Incident Response Plans (CIRP)	Respond to Cybersecurity Incidents	Total		
						f = ∑a,b,c,d,e		
	a	b	c	d	e	Undiscounted	Discounted at 3%	Discounted at 7%
1	$89.4	$35.8	$70.9	$71.5	$291.8	$559.4	$543.1	$522.8
2	$9.9	$3.9	$0.0	$0.4	$291.9	$306.2	$297.2	$286.1
3	$9.9	$4.0	$0.0	$0.4	$292.0	$306.4	$297.4	$286.3
4	$10.0	$4.0	$0.0	$0.4	$292.2	$306.5	$297.6	$286.5
5	$10.0	$4.0	$0.0	$0.4	$292.3	$306.8	$297.8	$286.7
6	$10.1	$4.0	$0.0	$0.5	$292.4	$307.0	$298.0	$286.9
7	$10.2	$4.1	$0.0	$0.5	$292.5	$307.2	$298.2	$287.1
8	$10.2	$4.1	$0.0	$0.5	$292.6	$307.4	$298.4	$287.3
9	$10.3	$4.1	$0.0	$0.5	$292.7	$307.6	$298.6	$287.5
10	$10.4	$4.1	$0.0	$0.5	$292.9	$307.8	$298.9	$287.7
Total						**$3,322.2**	**$3,225.4**	**$3,104.8**
Annualized							**$322.5**	**$310.5**

Note: Totals may not add due to rounding.

5.1.6 Total Cost Impacts of Alternative 1

As shown in Table 5-9, the total cumulative cost impacts over ten-years for this alternative are $111.2 million undiscounted and $79.4 million when discounted at 7 percent. This alternative costs $2,978.6 million less than the preferred alternative undiscounted and a $2,082.2 million less when discounted at 7 percent.

Table 5-9: Total Cost for All Requirements Including Implementation for Alternative 1 - Industry and TSA ($ Thousands)

Year	Industry				Total Regulated Industries Cost	TSA	Total Cost		
	Pipelines	Freight Rail	PTPR	OTRB			g = ∑e,f		
	a	b	c	d	e	f	Undiscounted	Discounted at 3%	Discounted at 7%
1	$10,353.8	$3,677.8	$1,492.3	$188.5	$15,712.4	$559.4	$16,271.8	$15,797.8	$15,207.2
2	$7,203.2	$1,997.6	$891.4	$6.0	$10,098.1	$306.2	$10,404.3	$9,807.1	$9,087.5
3	$7,203.2	$2,013.0	$911.2	$6.1	$10,133.5	$306.4	$10,439.9	$9,554.0	$8,522.1
4	$7,203.2	$2,028.8	$930.8	$6.3	$10,169.1	$306.5	$10,475.7	$9,307.5	$7,991.8
5	$7,203.2	$2,045.0	$951.5	$6.4	$10,206.1	$306.8	$10,512.9	$9,068.5	$7,495.5
6	$7,203.2	$2,060.9	$972.2	$6.6	$10,242.9	$307.0	$10,549.8	$8,835.3	$7,029.8
7	$7,203.2	$2,076.8	$993.5	$6.8	$10,280.3	$307.2	$10,587.4	$8,608.6	$6,593.3
8	$7,203.2	$2,093.2	$1,015.3	$6.9	$10,318.7	$307.4	$10,626.1	$8,388.3	$6,184.5
9	$7,203.2	$2,109.4	$1,037.3	$7.1	$10,357.1	$307.6	$10,664.7	$8,173.6	$5,800.9
10	$7,203.2	$2,126.1	$1,060.3	$7.3	$10,396.9	$307.8	$10,704.7	$7,965.3	$5,441.7
Total	**$75,182.6**	**$22,228.6**	**$10,255.8**	**$247.9**	**$107,915.0**	**$3,322.2**	**$111,237.2**	**$95,505.9**	**$79,354.4**
Annualized								**$11,196.2**	**$11,298.3**

Note: Totals may not add due to rounding.

TSA has not selected this alternative because although it has a smaller estimated cost, it also provides a reduced level of risk mitigation. This alternative would provide TSA oversight in terms of awareness for both "response" and "recovery" to a cybersecurity incident as described by NIST, but it does not include visibility or accountability of any "detect" or "protect" elements that owner/operators need to implement as part of a cyber-risk management program in order to prevent malicious actors from exploiting vulnerabilities as well as to ensure the confidentiality, availability, integrity of their critical systems.[422] The exposure of cyber threats, such as ransomware, phishing, malware, third-party risks, internal risks, compliance failures, is a consequence of increase use of technology that relies on connectivity and interconnectivity between IT and OT, where convenience is sometimes in tension with security practices. Thus, not including detect and protect elements, such as protecting critical cyber systems and having capabilities to respond to a cybersecurity incident identified in the rule, reduces the level of protection when compared to the preferred alternative. For instance, absent some of the defensive postures set forth in this proposed rule, that deal with protection of critical cyber systems, a malicious actor could launch a successful phishing attack. The measures in Alternative 1 would result in the owner/operators being reactionary after an attack, versus enabling early detection and mitigation of an attack's impact, which is the goal of the provisions of the preferred alternative.

Furthermore, the lack of proactive planning and associated visibility/accountability provided by the omitted elements also leaves owner/operators less secure. Conducting a cybersecurity

---

[422] See NIST Cybersecurity Framework core functions (identify, protect, detect, respond, recover). Available at https://www.nist.gov/cyberframework/online-learning/cybersecurity-framework-components. Accessed July 24, 2023.

evaluation, developing a cybersecurity operational implementation plan, and implementing a cybersecurity assessment plan provide tools to measure and understand one's risk, have a plan to mitigate against that risk, and evaluate whether the plan is effective.

Other proactive measures that help mitigate risk include providing cybersecurity training and designating an accountable executive to oversee and advocate for cybersecurity related efforts. For example, to reduce cybersecurity risks caused by human error, cybersecurity training (part of detection) can help raise awareness of common incidents and the methods to identify and prevent them. Identification of an accountable executive fosters efficiency and cybersecurity support to advocate for the tools and resources necessary to address cybersecurity issues, identify trends impacting the organization, and ultimately optimize risk reduction, value, and costs.

In order to stay ahead of today's evolving threat landscape and to be prepared for all forms of cyber-incidents, owner/operators must implement appropriate security measures/controls and optimize their processes to ensure cyber resilience and improve their ability to detect and mitigate cyber risks as supported by the requirements of the rule. This is especially relevant for owner/operators where a cybersecurity incident could not only impact their operations, but have cascading national implications.

TSA believes a multi-faceted approach toward reducing risk related to cybersecurity is necessary, given the key role owner/operators play in the supply chain, movement of people and goods, and the economy as a whole as they face the dynamic and emerging cybersecurity threats to the Nation's surface transportation systems.

5.2 Alternative 2: Applicability Adjustment

This alternative would adjust the applicability of the requirements to cover a smaller portion of

owner/operators in each of the regulated industries, aside from OTRB, who would still be subject to the same reporting requirements as in the preferred alternative. All of the preferred alternative rule provisions would still apply to this reduced population. Specifically, this alternative would reduce the freight rail applicability to cover a population limited to only Class I freight rail lines as defined by the Surface Transportation Board, resulting in only six owner/operators being impacted versus 73 in the preferred alternative. The PTPR applicability would cover owner/operators who host Class 1 freight rail lines or those who have an average daily ridership of 100,000 passengers in any of the previous three years or at any time in the future. This covers 27 of the 34 owner/operators in the preferred alternative. For the regulated pipeline owner/operators, applicability would cover the 98 most critical owner/operators of hazardous liquid and natural gas pipelines and liquefied natural gas facilities as determined by TSA.

5.2.1 Cost Impacts of Alternative 2 on Freight Rail Entities

This alternative would reduce the cost impact on freight rail entities relative to the preferred alternative. Alternative 2 would adjust the applicability of the proposed rule discussed in Section 2.1.1 from 73 entities to only the 6 entities designated as Class 1 (which represent the largest carriers, by revenue).[423] In this alternative, all of the proposed rule's requirements would remain the same, including from sections 1580.301 through 1580.331. This alternative makes no other changes relative to the proposed rule. Thus, the cost impact for the remaining 6 entities would be equivalent to the cost per owner/operator under the proposed rule. As a result of this change to the number of in-scope entities, the number of employees adjust from 116,960 in Year 1 of the

[423] These 6 Class 1 railroads are currently covered by the SDs.

preferred alternative to 97,606 in Alternative 2. Table 5-10 shows the total costs for freight rail under the Alternative 2 requirements.

Table 5-10: Total Costs for Alternative 2 Requirements - Freight Rail ($ Thousands)

Year	Familiarization	CRM Program				Reporting Cybersecurity Incidents	CIRP	Total Cost		
		CSE	COIP	CAP	Record-keeping and Compliance			h = ∑a,b,c,d,e,f,g		
	a	b	c	d	e	f	g	Undiscounted	Discounted at 3%	Discounted at 7%
1	$12.4	$19.2	$44,479.9	$70.3	$22.7	$0.1	$161.4	$44,766.0	$43,462.1	$41,837.4
2	$0.0	$19.2	$44,362.6	$206.1	$22.7	$0.1	$115.6	$44,726.2	$42,158.7	$39,065.6
3	$0.0	$19.2	$44,562.6	$70.3	$22.7	$0.1	$115.6	$44,790.4	$40,989.6	$36,562.3
4	$0.0	$19.2	$44,757.5	$206.1	$22.7	$0.1	$115.6	$45,121.1	$40,089.5	$34,422.7
5	$0.0	$19.2	$44,960.0	$70.3	$22.7	$0.1	$115.6	$45,187.9	$38,979.5	$32,218.3
6	$0.0	$19.2	$45,163.9	$206.1	$22.7	$0.1	$115.6	$45,527.5	$38,128.6	$30,336.9
7	$0.0	$19.2	$45,369.1	$70.3	$22.7	$0.1	$115.6	$45,596.9	$37,074.5	$28,395.5
8	$0.0	$19.2	$45,575.6	$206.1	$22.7	$0.1	$115.6	$45,939.2	$36,264.8	$26,737.0
9	$0.0	$19.2	$45,783.4	$70.3	$22.7	$0.1	$115.6	$46,011.3	$35,263.8	$25,027.1
10	$0.0	$19.2	$45,992.7	$206.1	$22.7	$0.1	$115.6	$46,356.3	$34,493.4	$23,565.2
Total	**$12.4**	**$191.7**	**$451,007.2**	**$1,381.7**	**$227.2**	**$0.8**	**$1,201.7**	**$454,022.8**	**$386,904.5**	**$318,168.0**
Annualized									**$45,357.0**	**$45,300.0**

Note: Totals may not add due to rounding.

5.2.2 Cost Impacts of Alternative 2 on Passenger Transit and Passenger Rail Entities

This alternative would reduce the cost impact on PTPR entities relative to the preferred alternative. Alternative 2 would adjust the applicability of the proposed rule discussed in Section 2.1.2 from 34 entities to 27 entities based on adjusted applicability criteria. The adjusted applicability criteria covers a limited population of only those entities which host Class 1 freight rail lines or those who have an average daily ridership of 100,000 passengers in the previous 5 years or at any time in the future. In this alternative, all of the proposed rule's requirements would remain the same, including from sections 1582.201 through 1582.231. This alternative makes no other changes relative to the proposed rule. Thus, the cost impact for the remaining 27 entities would be equivalent to the cost per owner/operator under the proposed rule. As a result of this change to the number of in-scope entities, the number of employees adjust from 374,600 in Year 1 of the preferred alternative to 334,936 in Alternative 2. Table 5-11 shows the total costs for PTPR under the Alternative 2 requirements.

Table 5-11: Total Costs for Alternative 2 Requirements - PTPR ($Thousands)

Year	Familiarization	CRM Program				Reporting Cyber-security Incidents	CIRP	Total Cost		
		CSE	COIP	CAP	Record-keeping and Compliance			h = ∑a,b,c,d,e,f,g		
	a	b	c	d	e	f	g	Undiscounted	Discounted at 3%	Discounted at 7%
1	$38.5	$82.0	$104,473.6	$308.7	$66.9	$1.0	$692.0	$105,662.8	$102,585.2	$98,750.3
2	$0.8	$83.8	$104,769.1	$924.0	$68.4	$1.0	$535.7	$106,382.9	$100,276.1	$92,918.9
3	$0.9	$85.7	$106,153.3	$335.8	$69.9	$1.0	$547.6	$107,194.1	$98,097.8	$87,502.3
4	$0.9	$87.5	$107,526.4	$951.7	$71.4	$1.1	$559.4	$109,198.3	$97,021.3	$83,306.9
5	$0.9	$89.4	$108,955.8	$363.7	$72.9	$1.1	$571.6	$110,055.5	$94,934.9	$78,468.1
6	$0.9	$91.4	$110,412.7	$980.5	$74.6	$1.1	$584.3	$112,145.5	$93,920.1	$74,727.3
7	$0.9	$93.4	$111,893.4	$393.3	$76.2	$1.1	$597.1	$113,055.5	$91,924.4	$70,405.3
8	$1.0	$95.4	$113,398.9	$1,010.6	$77.9	$1.2	$610.1	$115,195.0	$90,936.0	$67,044.5
9	$1.0	$97.5	$114,934.0	$424.0	$79.6	$1.2	$623.5	$116,160.7	$89,027.5	$63,183.7
10	$1.0	$99.7	$116,494.6	$1,042.1	$81.3	$1.2	$637.1	$118,356.9	$88,068.6	$60,166.6
Total	**$46.8**	**$906.0**	**$1,099,011.8**	**$6,734.4**	**$738.9**	**$11.1**	**$5,958.3**	**$1,113,407.2**	**$946,791.9**	**$776,473.9**
Annualized									**$110,992.9**	**$110,552.4**

Note: Totals may not add due to rounding.

5.2.3 Cost Impacts of Alternative on Over the Road Bus Entities

This alternative does not change the cost impact on OTRB entities relative to the preferred alternative as all owner/operators who are in-scope in the preferred alternative remain covered under Alternative 2. In Alternative 2, all of the proposed rule's requirements would remain the same, including from sections 1584.101 through 1584.115. This alternative makes no other changes relative to the preferred alternative. Thus, the cost impact for all entities would be equivalent to the cost under the proposed rule.

5.2.4 Cost Impacts of Alternative 2 on Pipeline Entities

This alternative would reduce the cost impact on pipeline entities relative to the preferred alternative. Alternative 2 would adjust the applicability of the proposed rule discussed in Section 2.1.4 from the proposed population of 115 entities based on adjusted applicability criteria. The adjusted applicability criteria covers a limited population of the 98 most critical owner/operators of hazardous liquid and natural gas pipelines and liquefied natural gas facilities.[424] In this alternative, all of the proposed rule's requirements would remain the same, including from sections 1586.201 through 1586.231. This alternative makes no other changes relative to the proposed rule. Thus, the cost impact for the remaining 98 entities would be equivalent to the cost per owner/operator under the proposed rule. As a result of this change to the number of in-scope entities, the number of employees adjust from 49,900 in Year 1 of the preferred alternative to 42,523 in Alternative 2. Table 5-12 shows the total costs for pipelines under the Alternative 2 requirements.

[424] These pipeline entities are currently covered by the SDs.

Table 5-12: Total Costs for Alternative 2 Requirements - Pipelines ($ Thousands)

Year	Familiarization	Physical Security Costs	CRM Program				Reporting Cyber-security Incidents	CIRP	Total Cost		
			CSE	COIP	CAP	Record-keeping and Compliance			i = ∑a,b,c,d,e,f,g,h		
	a	b	c	d	e	f	g	h	Undiscounted	Discounted at 3%	Discounted at 7%
1	$312.6	$28.9	$829.3	$63,729.0	$1,158.3	$549.3	$32.2	$5,868.5	$72,508.2	$70,396.3	$67,764.7
2	$0.0	$16.5	$829.3	$59,224.4	$3,373.6	$549.3	$32.2	$5,174.1	$69,199.5	$65,227.1	$60,441.5
3	$0.0	$16.5	$829.3	$59,743.7	$1,158.3	$549.3	$32.2	$5,174.1	$67,503.5	$61,775.2	$55,102.9
4	$0.0	$16.5	$829.3	$60,170.5	$3,373.6	$549.3	$32.2	$5,174.1	$70,145.5	$62,323.4	$53,513.7
5	$0.0	$16.5	$829.3	$60,709.3	$1,158.3	$549.3	$32.2	$5,174.1	$68,469.0	$59,062.0	$48,817.5
6	$0.0	$16.5	$829.3	$61,258.0	$3,373.6	$549.3	$32.2	$5,174.1	$71,233.1	$59,656.6	$47,465.6
7	$0.0	$16.5	$829.3	$61,817.0	$1,158.3	$549.3	$32.2	$5,174.1	$69,576.7	$56,572.2	$43,328.9
8	$0.0	$16.5	$829.3	$62,386.5	$3,373.6	$549.3	$32.2	$5,174.1	$72,361.5	$57,122.8	$42,115.1
9	$0.0	$16.5	$829.3	$62,966.5	$1,158.3	$549.3	$32.2	$5,174.1	$70,726.3	$54,205.8	$38,470.4
10	$0.0	$16.5	$829.3	$63,557.5	$3,373.6	$549.3	$32.2	$5,174.1	$73,532.6	$54,715.1	$37,380.2
Total	**$312.6**	**$177.3**	**$8,292.8**	**$615,562.5**	**$22,659.5**	**$5,493.2**	**$322.5**	**$52,435.4**	**$705,255.8**	**$601,056.6**	**$494,400.4**
Annualized										**$70,462.2**	**$70,391.5**

Note: Totals may not add due to rounding.

5.2.5 Cost Impacts of Alternative 2 on TSA

Alternative 2 would reduce the cost impact on TSA relative to the preferred alternative. This alternative would require TSA review fewer plans and respond to fewer incidents than what is currently proposed for industry modes. For those entities that the rule remains applicable, TSA's unit costs would be equivalent to the cost under the primary proposal. Table 5-13 shows the total costs for TSA under the Alternative 2 requirements.

Table 5-13: Total Costs for Alternative 2 Requirements - TSA ($ Thousands)

Year	Physical Security Costs	CRM Program			CIRP	Total Costs		
		CSE	COIP	CAP		f = ∑a,b,c,d,e		
	a	b	c	d	e	Undiscounted	Discounted at 3%	Discounted at 7%
1	$63.9	$42.2	$2,645.5	$337.6	$209.2	$3,298.4	$3,202.3	$3,082.6
2	$63.9	$42.4	$1,458.2	$339.1	$167.3	$2,070.9	$1,952.0	$1,808.8
3	$63.9	$42.6	$1,458.5	$340.7	$167.4	$2,073.1	$1,897.2	$1,692.3
4	$63.9	$42.8	$400.3	$342.3	$167.6	$1,016.8	$903.4	$775.7
5	$63.9	$43.0	$400.6	$343.9	$167.7	$1,019.1	$879.1	$726.6
6	$63.9	$43.2	$400.9	$345.6	$167.9	$1,021.4	$855.4	$680.6
7	$63.9	$43.4	$401.1	$347.3	$168.0	$1,023.7	$832.4	$637.5
8	$63.9	$43.6	$401.4	$349.0	$168.1	$1,026.1	$810.0	$597.2
9	$63.9	$43.8	$401.7	$350.8	$168.3	$1,028.5	$788.3	$559.4
10	$63.9	$44.1	$402.0	$352.6	$168.4	$1,031.0	$767.2	$524.1
Total	**$638.8**	**$431.1**	**$8,370.2**	**$3,449.0**	**$1,720.0**	**$14,609.0**	**$12,887.2**	**$11,084.9**
Annualized							**$1,510.8**	**$1,578.2**

Note: Totals may not add due to rounding.

5.2.6 Total Cost Impacts of Alternative 2

As shown in Table 5-14 the total cumulative cost impacts over ten years for this alternative are $2,287.5 million undiscounted and $1,600.3 million when discounted at 7 percent. This alternative costs $802.3 million less than the primary proposal undiscounted and a $561.2 million less when discounted at 7 percent.

Table 5-14: Total Cost for All Requirements Including Implementation for Alternative 2 - Industry and TSA ($ Thousands)

Year	Industry					TSA	Total Cost		
	Pipelines	Freight Rail	PTPR	OTRB	Total Regulated Industries Cost		g = ∑e,f		
	a	b	c	d	e	f	Undiscounted	Discounted at 3%	Discounted at 7%
1	$72,508.2	$44,766.0	$105,662.8	$188.5	$223,125.4	$3,298.4	$226,423.9	$219,829.0	$211,611.1
2	$69,199.5	$44,726.2	$106,382.9	$6.0	$220,314.5	$2,070.9	$222,385.4	$209,619.6	$194,240.0
3	$67,503.5	$44,790.4	$107,194.1	$6.1	$219,494.1	$2,073.1	$221,567.2	$202,765.4	$180,864.8
4	$70,145.5	$45,121.1	$109,198.3	$6.3	$224,471.3	$1,016.8	$225,488.1	$200,343.2	$172,023.8
5	$68,469.0	$45,187.9	$110,055.5	$6.4	$223,718.9	$1,019.1	$224,738.0	$193,861.0	$160,235.1
6	$71,233.1	$45,527.5	$112,145.5	$6.6	$228,912.7	$1,021.4	$229,934.1	$192,566.2	$153,214.8
7	$69,576.7	$45,596.9	$113,055.5	$6.8	$228,235.8	$1,023.7	$229,259.5	$186,409.0	$142,771.3
8	$72,361.5	$45,939.2	$115,195.0	$6.9	$233,502.6	$1,026.1	$234,528.7	$185,139.1	$136,497.8
9	$70,726.3	$46,011.3	$116,160.7	$7.1	$232,905.4	$1,028.5	$233,933.9	$179,290.9	$127,244.5
10	$73,532.6	$46,356.3	$118,356.9	$7.3	$238,253.1	$1,031.0	$239,284.0	$178,049.8	$121,639.9
Total	**$705,255.8**	**$454,022.8**	**$1,113,407.2**	**$247.9**	**$2,272,933.7**	**$14,609.0**	**$2,287,542.7**	**$1,947,873.0**	**$1,600,343.1**
Annualized								**$228,350.1**	**$227,852.9**

Note: Totals may not add due to rounding.

TSA has not selected this alternative despite estimated cost savings compared to the preferred alternative, because it does not cover owner/operators who play a critical role in contributing to the stability and security of the movement of people and goods. An incident on such owner/operators may still result in a ripple effect throughout the economy. The preferred alternative would encompass those entities that are responsible for transporting a) the greatest volumes of cargo; b) the greatest number of people; and c) providing vital links for the delivery of essential products for national defense.

Reducing applicability to just Class 1 railroads would not mitigate risks for those entities not covered and would result in the reduction of security of the freight rail sector as a whole. This is because Class 2 and 3 railroads account for about 33 percent of freight rail mileage and often the first and last mile rail for pickup and delivery service.[425] Reducing the scope of covered entities will decrease the effectiveness of the rule. Although individual Class 2 and 3 railroads may not individually have an outsized effect on the overall rail network, Class 2 and 3 railroads are vital to the flow of freight, commodities, and military hardware across the Nation's rail system. They also provide port, terminal switching, and inter-railroad transfer services for the Class 1 railroads at critical points in major metropolitan areas. This interconnectedness between railroads is a critical facet of the Nation's overall railroad industry. Leaving Class 2 and 3 railroads out of the applicability pool may leave the previously discussed sections of rail vulnerable to cybersecurity incidents. This would have ramifications for owner/operators transporting critical materials and due to the interconnectedness of the Nation's rail system, the degradation of one or more of these

[425] Association of American Railroads (AAR). Jul. 2023. Freight Rail Facts & Figures: Capacity and Service. https://www.aar.org/facts-figures#4-capacity-amp-service. Accessed on July 30, 2023.

Class 2 & 3 railroads could have a cascading effect across the rail network which would affect the system as a whole and potentially immobilize a significant proportion of Class 1 railroads. Critical operations that would not be covered under this alternative include Class 2 and 3 railroads that provide services to multiple Class I railroads, serves as a host railroad for higher risk passenger rail operations, operate over 400,000 train miles, transport Rail Security-Sensitive Materials in High Threat Urban Areas, or are designated as a Defense Connector Railroad by DoD.

For PTPR, the criteria of the preferred alternative apply to the highest consequence operators and cover most of the national daily rail ridership. The rail transit entities and passenger railroads excluded in this alternative represent average daily ridership of 935.6 thousand per day,[426] and provide critical support to major urban areas and allow for people to travel to work and support the local and regional economy. By limiting the covered population, this portion of the commuting population could be exposed to an increased level of risk. If a successful cyberattack was perpetrated against one of these entities, the damages and consequences could have a cascading effect beyond just the targeted entity into the local community. Similar to the freight rail network, the interconnected nature of the national rail system means that an attack on one entity could affect other covered entities in the same locality or region. If covered entities become immobilized due to such an attack, it could have a spillover effect on Class 1 freight rails given that many passenger railroads also host Class 1 freight rail entities on their tracks.

[426] In the preferred alternative, covered entities service an average of 15,677,255 riders per day while under alternative 2, the covered entities service an average of 14,741,680 riders per day from the remaining owner/operators. The non-covered owner/operators from Alternative 2 account for 935,575 in average daily ridership.

Akin to the other modalities, a reduction in covered pipeline operators would result in an increased level of risk. This increased risk could result in a successful attack that results in operational disruption with potential widespread impacts or implications. The pipeline operators excluded in this alternative provide critical support to major urban centers, such as liquefied natural gas (LNG) operators providing service during peak demand times. Since even a minor disruption in a pipeline system may result in product shortages, a cyber incident that disrupts this service could lead to significant hardship for the consumers, both individual and commercial, who rely on LNG for heating during the winter months. Another example stemming from reduced applicability is a successful cyberattack against a control room that operates multiple pipeline systems could lead to cascading impact on pipeline delivery. This would disrupt the accessibility of needed product to locations throughout the country and potentially result in a significant impact to the communities reliant on the pipeline product.

Therefore, based on the reasons discussed above, TSA believes reducing the population covered for each mode, fails to mitigate risk for entities whose impact may be severe and could result in cascading impacts through the larger transportation systems and economy. Nonetheless, TSA requests public comment on the different applicability requirements including associated benefits and costs.

5.3 Alternative 3: Addition of a Vetting Requirement

In addition to the requirements in the proposed rule, Alternative 3 would introduce a requirement for accountable executives and cybersecurity coordinators of all covered entities, as well as pipeline physical security coordinators, to undergo a Level 3 Security Threat Assessment (STA). A Level 3 STA includes a terrorism/other analyses check, immigration check, and a criminal history records check (CHRC). 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 employees in the Security Vetting of Certain Transportation Workers Rulemaking.[427] A Level 2 STA includes a terrorism/other analyses check and immigration check.

The primary benefit of this alternative is its potential to reduce insider threats from employees who may wish to do harm. 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 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.

5.3.1 STA Costs

This section discusses TSA's estimates on an individual's cost to undergoing an STA. Costs include an individual's opportunity cost of time, STA fees, and travel expenses which are used to generate STA unit costs for this analysis. There are also additional vetting-related costs (e.g., disqualification costs) that are discussed qualitatively. In this Alternative, TSA leverages the methodology and fees from the Security Vetting of Certain Transportation Workers Notice of Proposed Rulemaking. [428]

5.3.1.1 Opportunity Costs

The opportunity cost of individuals undergoing an STA relates to the time spent providing

[427] NPRM: Surface Vetting Preliminary Regulatory Impact Analysis and Initial Regulatory Flexibility Analysis. Document ID TSA-2023-0001-0004. May 25, 2023. https://www.regulations.gov/document/TSA-2023-0001-0004.
[428] NPRM: Surface Vetting Preliminary Regulatory Impact Analysis and Initial Regulatory Flexibility Analysis. Document ID TSA-2023-0001-0004. May 25, 2023. https://www.regulations.gov/document/TSA-2023-0001-0004.

biographic (e.g., name, address, and date of birth) and biometric (e.g., fingerprints) information to TSA online and/or at TSA's enrollment centers. Enrollment time burdens include a combination of an applicant's time spent providing biographic information, completing identity assurance, providing fingerprints (if necessary), scanning immigration documents, commuting to and from a TSA enrollment center, and the wait time at the enrollment center. Overall, based on its experience with other vetting programs, TSA estimates the total time burden to complete an initial STA application to be 85.8 minutes (1.43 hours) for frontline employees and 90.8 minutes (1.51 hours) for physical and cybersecurity coordinators and accountable executives who would also have to submit fingerprints.[429] In addition to an initial standard enrollment, some individuals may have a comparable STA and would use their STA to meet the vetting requirement. TSA assumes a ten-minute (0.167 hours) burden for individuals with a comparable STA to provide their biographic data capture.[430]

All STAs administered by TSA are typically valid for up to five-years from issuance. For renewals, TSA estimates a five-minute (0.083 hours) time burden for online renewals and comparable STA holders, as well as 62.5 minutes for in-person renewals.[431] Table 5-15 displays the different time burdens for the initial standard and comparable enrollments as well as renewals.

[429] Id at 66.
[430] Ibid.
[431] Id.at. 67.

Table 5-15: STA Enrollment Time Burdens for Frontline Employees, Cybersecurity Coordinators, and Accountable Executives

Enrollment Component	Enrollment Time Burden (Hours)				
	Standard Enrollment (Initial)		Comparable (Initial)	In-Person Renewals	Online & Comparable Renewals
	Frontline Employees	Coordinators & Accountable Executives	Frontline, Cybersecurity Coordinators & Accountable Executives		
STA Familiarization	0.083	0.083	0.083	-	-
Biographic Data Capture	0.222	0.222	0.083	0.083	0.083
Identity Assurance	0.019	0.019	-	0.019	-
Fingerprint Adjustment	-	0.084	-	-	-
Scan Immigration Documents	0.047	0.047	-	0.047	-
Wait at Enrollment Center	0.167	0.167	-	-	-
Round Trip to Enrollment Center	0.892	0.892	-	0.892	-
Applicant's Total Time Burden	**1.429**	**1.514**	**0.167**	**1.041**	**0.083**

Note: Totals may not add due to rounding.

TSA multiplies each labor category's compensation rate with the respective time burden to calculate the opportunity cost for frontline employees, physical and cybersecurity coordinators, and accountable executives. In Alternative 3, TSA uses a single compensation rate of $155.07 for Level 3 STA applicants, consisting of physical security coordinators, cybersecurity coordinators, and accountable executives.[432] For Level 2 STA applicants, TSA uses the pipeline frontline employee compensation rate, calculated in Section 2.3.4, of $69.32 per hour.

[432] TSA calculated a simple average wage rate for Level 3 STA applicants using the compensation rates for freight rail cybersecurity coordinators ($127.10) and accountable executives ($202.60), PTPR cybersecurity coordinators ($105.82) and accountable executives ($134.31), and pipeline cybersecurity coordinators ($118.09), accountable executives ($267.30), and physical security coordinators ($130.24) which are described in Section 2.3 of this RIA. $155.07 Compensation Rate for Level 3 STA Applicants = ($127.10 + $202.60 + $105.82 + $134.31 + $118.09 + $267.30 + $130.24) ÷ 7 labor categories across all modes.

Table 5-16: Opportunity Costs for Frontline Employees, Coordinators, and Accountable Executives

Enrollment	Affected Individuals	Hourly Compensation Rate	STA Time Burdens (Hours)	Opportunity Costs
		a	b	c = a x b
Standard Enrollment (Initial)	Frontline Employees	$69.32	1.426	$98.86
	Physical & Cybersecurity Coordinators and Accountable Executives	$155.07	1.510	$234.22
Comparable (Initial)	Frontline Employees	$69.32	0.160	$11.09
	Physical & Cybersecurity Coordinators and Accountable Executives	$155.07		$24.81
In-Person Renewal	Frontline Employees	$69.32	1.038	$71.93
	Physical & Cybersecurity Coordinators and Accountable Executives	$155.07		$160.90
Online and Comparable Renewals	Frontline Employees	$69.32	0.080	$5.55
	Physical & Cybersecurity Coordinators and Accountable Executives	$155.07		$12.41

Note: Totals may not add due to rounding.

5.3.1.2 STA Fees

TSA assumes the affected population of this alternative would incur the same fees estimated for other surface modes of transportation.[433] For a Level 2 STA, the initial in-person enrollment and in-person renewal fee is $66, the online renewal fee is $41, and the comparable STA fee is $30. For a Level 3 STA, the initial in-person enrollment fee is $87, in-person renewal fee is $76, online renewal is $51, and comparable STA fee is $30.

5.3.1.3 Travel Expenses

TSA accounts for travel costs incurred by individuals seeking to obtain an STA using an

[433] TSA leverages the methodology and fees from the Security Vetting of Certain Transportation Workers NPRM for this alternative. See NPRM: Surface Vetting Preliminary Regulatory Impact Analysis and Initial Regulatory Flexibility Analysis. Document ID TSA-2023-0001-0004. May 25, 2023. P. 73. https://www.regulations.gov/document/TSA-2023-0001-0004

estimated average round trip travel distance of 50.32 miles to an enrollment center.[434] TSA multiplies this distance by the General Services Administration privately owned automobile reimbursement rate of $0.625 per mile to calculate a travel cost of $31.45 per individual trip for this analysis.[435]

5.3.1.4 STA Unit Cost

Table 5-17 presents the resulting individual unit STA cost by type and enrollment. Specifically, TSA sums the individual's opportunity cost, STA fee, and travel expense (if applicable) to estimate a total unit STA cost per individual for Level 2 (frontline employees) and Level 3 STAs (physical and cybersecurity coordinators, and accountable executives).

Table 5-17: Unit STA Costs by Type and Enrollment

	Initial In-Person	Initial Comparable	In-Person Renewal	Online Renewal	Comparable Renewal
Level 2 STA					
STA Fee	$66.00	$30.00	$66.00	$41.00	$30.00
Opportunity Cost	$98.86	$11.09	$71.93	$5.55	$5.55
Travel Cost	$31.45	N/A	$31.45	N/A	N/A
Total	**$196.31**	**$41.09**	**$169.38**	**$46.55**	**$35.55**
Level 3 STA					
STA Fee	$87.00	$30.00	$76.00	$51.00	$30.00
Opportunity Cost	$234.22	$24.81	$160.90	$12.41	$12.41
Travel Cost	$31.45	N/A	$31.45	N/A	N/A
Total	**$352.67**	**$54.81**	**$268.35**	**$63.41**	**$42.41**

Note: Totals may not add due to rounding.

5.3.2 Additional Vetting Related Costs

In addition to the STA unit cost, which is the primary cost of introducing the vetting requirement, owner/operators and employees would incur a number of additional costs which are

[434] TSA derived this distance by multiplying the average round-trip travel time to a TSA enrollment center (0.89 hours) by the average speed traveled on major U.S. arterials (56.41 mph). U.S. Department of Transportation, National Highway Traffic Safety Administration. Traffic Technology Series. Table 1: Overall Speed Estimates (in MPH) by Road Class (Free-Flow) https://www.nhtsa.gov/sites/nhtsa.gov/files/traffic_tech/812489_tt-national-traffic-speeds-survey-iii-2015.pdf. Accessed June 29, 2021. TSA uses the 2015 mean speed for major arterials.

[435] General Services Administration. Privately Owned Vehicle Mileage Reimbursement Rate, as of July 1, 2022. https://www.gsa.gov/travel/plan-book/transportation-airfare-pov-etc/privately-owned-vehicle-mileagerates/pov-mileage-rates-archived. Accessed July 25, 2023.

discussed qualitatively below.

First, owner/operators may incur additional time burdens associated with familiarizing themselves with the STA process, in addition to the requirements in the proposed rule. Some entities may also incur costs to update their management policies and other related administrative tasks as a result of the vetting requirement. In addition, owner/operators would incur recordkeeping costs to generate and maintain records related to their employees' STAs and to make those records available to TSA upon request at times of compliance inspections. As a result, compliance inspections may take longer than the inspections in the proposed rule as a result of spot checks to demonstrate STA compliance. Furthermore, owner/operators would incur costs to replace employees with unfavorable STAs, lost or diminished productivity costs resulting from the displaced individuals not performing their job, and hiring costs associated with restarting of the hiring process when a perspective new hire fails their initial STA.

Employees would also incur costs under Alternative 3 associated with redress if they have an unfavorable STA. Redress costs may include an individuals' opportunity cost, and attorney fees to request releasable materials; exchange information; and request appeals, waivers, review by administrative law judge, review by TSA Final Decision Maker, and judicial review. Employees who pass their STA would incur costs to update their contact information if it changes. Also, individuals required to undergo a CHRC would incur additional costs to report disqualifying crimes to TSA within 24 hours of occurrence.

5.3.3 STA Cost by Industry

In this section, TSA first calculates the ten-year total STA costs for pipeline frontline employees, pipeline physical security coordinators as well as cybersecurity coordinators and accountable

executives for all modes covered under this alternative. It then combines the STA costs with preferred alternative costs to estimate the alternative's total cost.

5.3.3.1 Freight Rail

The number of freight rail entities under Alternative 3 would be the same as those under the proposed rule. To calculate the ten-year number of STAs for cybersecurity coordinators and accountable executives in the freight rail industry, TSA leverages the initial population, growth (0.85 percent), and turnover (4.00 percent) presented in Section 2.2. Table 5-18 presents estimated new STAs from growth and turnover plus five-year renewals for total number of annual STAs as well as an estimate on the comparable STAs.[436]

As discussed in Section 3.1.3.2, TSA estimates all freight rail entities would designate one cybersecurity coordinator, one alternate, and one accountable executive for a total of three individuals. For growth, TSA assumes each new entity would add two new cybersecurity coordinators and alternates and one new accountable executives to the population.[437]

[436] TSA uses internal data to estimate a 50.45 percent comparable rate for freight rail security coordinators and 5 percent in-person renewal rate.

[437] 219 Freight Rail Level 3 STA Applicants in Year 1 = 73 Entities × (1 Cybersecurity Coordinator + 1 Alternate Cybersecurity Coordinator + 1 Accountable Executive)

Table 5-18: Number of Freight Rail Cybersecurity Coordinators & Accountable Executive STAs Under Alternative 3

Year	Initial Population	Growth	Turnover	5-Year Renewals	Total Annual STAs	Total Comparable STAs
	a	$b_n = [a_1 \times (1 + 0.85\%)^n] - [a_1 \times (1 + 0.85\%)^{n-1}]$	$c_n = a_1 + (b_1{:}b_n) \times 4.00\%$	$d_n = e_{n-5} \times (1 - 4.00\%)^5$	$e = \sum a,b,c,d$	f = e x 50.45%
1	219.00	-	-	-	219.00	110.49
2	-	1.86	8.76	-	10.62	5.36
3	-	1.88	8.83	-	10.71	5.40
4	-	1.89	8.91	-	10.80	5.45
5	-	1.91	8.99	-	10.90	5.50
6	-	1.93	9.06	178.57	189.56	95.64
7	-	1.94	9.14	8.66	19.74	9.96
8	-	1.96	9.22	8.73	19.91	10.05
9	-	1.98	9.29	8.81	20.08	10.13
10	-	1.99	9.37	8.89	20.25	10.22
Total	**219**	**17**	**82**	**214**	**532**	**268**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed. Formulas with X_{yn-1} in year one are equal to the initial value of X_{y1}.

In Table 5-19, TSA presents the cybersecurity coordinator and accountable executive population for the freight rail industry based on STA type.

Table 5-19: Summary Table by STA Type for Freight Rail

Year	Initial Population (Non-Comparable)	In-Person Renewal (Non-Comparable)	Online Renewal (Non-Comparable)	Initial Comparable	Renewal Comparable
	a (Table 5-18, Column E – Column D) × 49.55%	b (Table 5-18, Column D) × 49.55% × 5.00%	c (Table 5-18, Column D) × 49.55% × 95.00%	d (Table 5-18, Column E – Column D) × 50.45%	e (Table 5-18, Column D × 50.45%
1	108.51	-	-	110.49	-
2	5.26	-	-	5.36	-
3	5.31	-	-	5.40	-
4	5.35	-	-	5.45	-
5	5.40	-	-	5.50	-
6	5.45	4.42	84.05	5.54	90.09
7	5.49	0.21	4.08	5.59	4.37
8	5.54	0.22	4.11	5.64	4.40
9	5.58	0.22	4.15	5.69	4.44
10	5.63	0.22	4.18	5.73	4.49
Total	**158**	**5**	**101**	**160**	**108**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

In Table 5-20, TSA calculates the total ten-year STA cost for freight rail under Alternative 3 by multiplying the number of cybersecurity coordinator and accountable executive STAs from

Table 5-19 by the respective STA unit costs presented in Table 5-17.

Table 5-20: STA Costs for Freight Rail Industry Under Alternative 3 ($ Thousands)

Year	In-Person Initial STA Cost	In-Person Renewal STA Cost	Online Renewal STA Cost	Initial Comparable STA Cost	Renewal Comparable STA Cost	Total STA Cost
	a (Table 5-19, Column A) × $352.67	b (Table 5-19, Column B) × $268.35	c (Table 5-19, Column C) × $63.41	d (Table 5-19, Column D) × $54.81	e (Table 5-19, Column E) × $42.41	f = ∑a,b,c,d,e
1	$38.3	-	-	$6.1	-	$44.3
2	$1.9	-	-	$0.3	-	$2.1
3	$1.9	-	-	$0.3	-	$2.2
4	$1.9	-	-	$0.3	-	$2.2
5	$1.9	-	-	$0.3	-	$2.2
6	$1.9	$1.2	$5.3	$0.3	$3.8	$12.6
7	$1.9	$0.1	$0.3	$0.3	$0.2	$2.7
8	$2.0	$0.1	$0.3	$0.3	$0.2	$2.8
9	$2.0	$0.1	$0.3	$0.3	$0.2	$2.8
10	$2.0	$0.1	$0.3	$0.3	$0.2	$2.8
Total	**$55.6**	**$1.4**	**$6.4**	**$8.8**	**$4.6**	**$76.7**

Note: Totals may not add due to rounding.

5.3.3.2 PTPR

The number of PTPR entities under Alternative 3 would be the same as those under the proposed rule. To calculate the ten-year number of STAs for cybersecurity coordinators and accountable executives in the PTPR industry, TSA leverages the initial population, growth (2.19 percent), and turnover (12.96 percent) presented in Section 2.2. TSA assumes all 34 PTPR affected entities would designate one cybersecurity coordinator, one alternate, and one accountable executive which equates to three individuals per entity and a total of 102 individuals. For growth, TSA assumes each new entity would add two new cybersecurity coordinators and alternates and one new accountable executives to the population.[438] Next, in Table 5-21, TSA calculates new STAs from growth and turnover plus five-year renewals for total number of annual STAs as well

[438] 102 PTPR Level 3 STA Applicants in Year 1 = 34 PTPR Agencies × (1 Cybersecurity Coordinator + 1 Alternate Cybersecurity Coordinator + 1 Accountable Executive).

as an estimate on comparable STAs.[439]

Table 5-21: Number of PTPR Cybersecurity Coordinators & Accountable Executive STAs Under Alternative 3

Year	Initial Population	Growth	Turnover	5-Year Renewals	Total Annual STAs	Total Comparable STAs
	a	$b_n = [a_1 \times (1 + 2.19\%)^n] - [a_1 \times (1 + 2.19\%)^{n-1}]$	$c_n = a_1 + (b_1{:}b_n) \times 12.96\%$	$d_n = e_{n-5} \times (1 - 12.96\%)^5$	$e = \sum a,b,c,d$	$f = e \times 47.32\%$
1	102.00	-	-	-	102.00	48.26
2	-	2.23	13.22	-	15.45	7.31
3	-	2.28	13.51	-	15.79	7.47
4	-	2.33	13.80	-	16.13	7.63
5	-	2.38	14.11	-	16.49	7.80
6	-	2.44	14.41	50.96	67.81	32.09
7	-	2.49	14.73	7.72	24.94	11.80
8	-	2.54	15.05	7.89	25.48	12.06
9	-	2.60	15.38	8.06	26.04	12.32
10	-	2.66	15.72	8.24	26.62	12.60
Total	**102**	**22**	**130**	**83**	**337**	**159**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed. Formulas with X_{yn-1} in year one are equal to the initial value of X_{y1}.

In Table 5-22, TSA presents the cybersecurity coordinator and accountable executive population for the PTPR industry based on STA type.

[439] TSA uses internal data to estimate a 47.32 percent comparable rate for PTPR security coordinators and a 5 percent in-person renewal rate.

Table 5-22: Summary Table by STA Type for PTPR

Year	Initial Population (Non-Comparable)	In-Person Renewal (Non-Comparable)	Online Renewal (Non-Comparable)	Initial Comparable	Renewal Comparable
	a (Table 5-21, Column E – Column D) × 52.68%	b (Table 5-21, Column D) × 52.68% × 5.00%	c (Table 5-21, Column D) × 52.68% × 95.00%	d (Table 5-21, Column E – Column D) × 47.32%	e (Table 5-21, Column D × 47.32%
1	53.74	-	-	48.26	-
2	8.14	-	-	7.31	-
3	8.32	-	-	7.47	-
4	8.50	-	-	7.63	-
5	8.69	-	-	7.80	-
6	8.88	1.34	25.50	7.97	24.11
7	9.07	0.20	3.86	8.15	3.65
8	9.27	0.21	3.95	8.32	3.73
9	9.47	0.21	4.03	8.51	3.81
10	9.68	0.22	4.12	8.70	3.90
Total	**134**	**2**	**41**	**120**	**39**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

In Table 5-23, TSA calculates the total ten-year STA cost for PTPR under Alternative 3 by multiplying the number of STAs presented in Table 5-22 by the STA unit costs presented in Table 5-17.

Table 5-23: STA Costs for PTPR Industry Under Alternative 3 ($ Thousands)

Year	In-Person Initial STA Cost	In-Person Renewal STA Cost	Online Renewal STA Cost	Initial Comparable STA Cost	Renewal Comparable STA Cost	Total STA Cost
	a (Table 5-22, Column A) × $352.67	b (Table 5-22, Column B) × $268.35	c (Table 5-22, Column C) × $63.41	d (Table 5-22, Column D) × $54.81	e (Table 5-22, Column E) × $42.41	f = ∑a,b,c,d,e
1	$19.0	-	-	$2.6	-	$21.6
2	$2.9	-	-	$0.4	-	$3.3
3	$2.9	-	-	$0.4	-	$3.3
4	$3.0	-	-	$0.4	-	$3.4
5	$3.1	-	-	$0.4	-	$3.5
6	$3.1	$0.4	$1.6	$0.4	$1.0	$6.6
7	$3.2	$0.1	$0.2	$0.4	$0.2	$4.1
8	$3.3	$0.1	$0.3	$0.5	$0.2	$4.2
9	$3.3	$0.1	$0.3	$0.5	$0.2	$4.3
10	$3.4	$0.1	$0.3	$0.5	$0.2	$4.4
Total	**$47.2**	**$0.6**	**$2.6**	**$6.6**	**$1.7**	**$58.6**

Note: Totals may not add due to rounding.

5.3.3.3 Pipelines

The number of pipeline entities under Alternative 3 would be the same as those under the proposed rule. To calculate the ten-year number of STAs for frontline employees in the pipeline industry, TSA leverages the initial population, growth (0.62 percent), and turnover (13.67 percent) presented in Section 2.2. As discussed in Section 2.1.4, TSA estimates a pipeline frontline employee estimate of 34,184 who perform security–sensitive functions. Next, in Table 5-24, TSA calculates the five-year renewals, total number of annual STAs, and comparable STAs.[440]

[440] TSA leverages an estimated 6.06 percent comparable rate for freight rail frontline employees, based on internal data, as a proxy for pipeline frontline employees and a 5 percent in-person renewal rate.

Table 5-24: Number of Pipeline Frontline Employee STAs Under Alternative 3

Year	Initial Population	Growth	Turnover	5-Year Renewals	Total Annual STAs	Total Comparable STAs
	a	$b_n = a_1 + (b_1{:}b_{n-1}) \times 0.62\%$	$c_n = a_1 + (b_1{:}b_{n-1}) \times 13.67\%$	$d_n = e_{n-5} \times (1 - 13.67\%)^5$	$e = \sum a,b,c,d$	f = e x 6.06%
1	34,184.00	-	-	-	34,184.00	2,071.71
2	-	211.94	4,672.95	-	4,884.89	296.05
3	-	213.25	4,701.92	-	4,915.17	297.88
4	-	214.58	4,731.08	-	4,945.66	299.73
5	-	215.91	4,760.41	-	4,976.32	301.59
6	-	217.25	4,789.92	16,391.99	21,399.16	1,296.89
7	-	218.59	4,819.62	2,342.41	7,380.62	447.30
8	-	219.95	4,849.50	2,356.93	7,426.38	450.07
9	-	221.31	4,879.57	2,371.55	7,472.43	452.86
10	-	222.68	4,909.82	2,386.26	7,518.76	455.67
Total	**34,184**	**1,955**	**43,115**	**25,849**	**105,103**	**6,370**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed. Formulas with X_{yn-1} in year one are equal to the initial value of X_{y1}.

In Table 5-25, TSA presents the frontline employee population for the pipeline industry based on STA type.

Table 5-25: Summary Table by STA Type for Pipeline Frontline Employees

Year	Initial Population (Non-Comparable)	In-Person Renewal (Non-Comparable)	Online Renewal (Non-Comparable)	Initial Comparable	Renewal Comparable
	a (Table 5-24, Column E – Column D) × 93.94%	b (Table 5-24, Column D) × 93.94%% × 5.00%	c (Table 5-24, Column D) × 93.94% × 95.00%	d (Table 5-24, Column E – Column D) × 6.06%	e (Table 5-24, Column D × 6.06%
1	32,112.29	-	-	2,071.71	-
2	4,588.84	-	-	296.05	-
3	4,617.29	-	-	297.88	-
4	4,645.93	-	-	299.73	-
5	4,674.73	-	-	301.59	-
6	4,703.71	769.93	14,628.63	303.46	993.43
7	4,732.87	110.02	2,090.43	305.34	141.96
8	4,762.22	110.70	2,103.38	307.23	142.84
9	4,791.74	111.39	2,116.43	309.14	143.73
10	4,821.45	112.08	2,129.56	311.05	144.62
Total	**74,451**	**1,214**	**23,068**	**4,803**	**1,567**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

In Table 5-26, TSA calculates the total ten-year STA cost for frontline employees in the pipeline industry under Alternative 3 by multiplying the number of STAs presented in Table 5-25 by the STA unit costs presented in Table 5-17.

Table 5-26: STA Costs for Pipeline Frontline Employees Under Alternative 3 ($ Thousands)

Year	In-Person Initial STA Cost	In-Person Renewal STA Cost	Online Renewal STA Cost	Initial Comparable STA Cost	Renewal Comparable STA Cost	Total STA Cost
	a (Table 5-25 Column A) × $196.31	b (Table 5-25, Column B) × $169.38	c (Table 5-25, Column C) × $46.55	d (Table 5-25, Column D) × $41.09	e (Table 5-25, Column E) × $35.55	f = ∑a,b,c,d,e
1	$6,303.8	-	-	$85.1	-	$6,389.0
2	$900.8	-	-	$12.2	-	$913.0
3	$906.4	-	-	$12.2	-	$918.6
4	$912.0	-	-	$12.3	-	$924.3
5	$917.7	-	-	$12.4	-	$930.1
6	$923.4	$130.4	$680.9	$12.5	$35.3	$1,782.5
7	$929.1	$18.6	$97.3	$12.5	$5.0	$1,062.6
8	$934.9	$18.8	$97.9	$12.6	$5.1	$1,069.2
9	$940.6	$18.9	$98.5	$12.7	$5.1	$1,075.8
10	$946.5	$19.0	$99.1	$12.8	$5.1	$1,082.5
Total	**$14,615.2**	**$205.6**	**$1,073.7**	**$197.4**	**$55.7**	**$16,147.6**

Note: Totals may not add due to rounding.

Next, to calculate the ten-year number of STAs for pipeline physical security coordinators, cybersecurity coordinators, and accountable executives, TSA leverages the initial population, growth (0 percent), and turnover (13.67 percent) presented in Section 2.2.

TSA estimates all pipeline entities would designate one cybersecurity coordinator, one alternate, one accountable executive, and approximately two physical security coordinators, per entity, for an approximate total of five individuals. This results in a total initial population of 606.[441] TSA assumes a 0 percent entity growth rate for pipelines; therefore, no new cybersecurity coordinators, accountable executives, or physical security coordinators would enter the population due to entity growth. Next, in Table 5-27, TSA calculates the five-year renewals, total number of annual STAs, and comparable STAs.[442]

[441] 606 Pipeline Level 3 STA Applicants in Year 1 = 115 Pipeline Agencies × (1 Cybersecurity Coordinator + 1 Alternate Cybersecurity Coordinator + 1 Accountable Executive + 2.27 Physical Security Coordinators).

[442] TSA leverages the 50.45 percent comparable rate for freight rail security coordinator and the 5 percent in-person renewal rate as a proxy for pipeline coordinators.

Table 5-27: Number of Pipeline Cybersecurity Coordinators, Physical Security Coordinators and Accountable Executives STAs Under Alternative 3

Year	Initial Population	Growth	Turnover	5-Year Renewals	Total Annual STAs	Total Comparable STAs
	a	$b_n = [a_1 \times (1 + 0.00\%)^n] - [a_1 \times (1 + 0.00\%)^{n-1}]$	$c_n = a_1 + (b_1{:}b_n) \times 13.67\%$	$d_n = e_{n-5} \times (1 - 13.67\%)^5$	$e = \sum a,b,c,d$	f = e x 50.45%
1	606.05	-	-	-	606.05	305.77
2	-	0	82.85	-	82.85	41.80
3	-	0	82.85	-	82.85	41.80
4	-	0	82.85	-	82.85	41.80
5	-	0	82.85	-	82.85	41.80
6	-	0	82.85	290.61	373.46	188.42
7	-	0	82.85	39.73	122.58	61.85
8	-	0	82.85	39.73	122.58	61.85
9	-	0	82.85	39.73	122.58	61.85
10	-	0	82.85	39.73	122.58	61.85
Total	**606**	**0**	**746**	**450**	**1801**	**909**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed. Formulas with X_{yn-1} in year one are equal to the initial value of X_{y1}.

In Table 5-28, TSA presents the cybersecurity coordinator, physical security coordinator, and accountable executive population for the pipeline industry based on STA type.

Table 5-28: Summary Table by STA Type for Pipeline Cybersecurity Coordinators, Physical Security Coordinators, and Accountable Executives

Year	Initial Population (Non-Comparable)	In-Person Renewal (Non-Comparable)	Online Renewal (Non-Comparable)	Initial Comparable	Renewal Comparable
	a (Table 5-27, Column E – Column D) × 49.55%	b (Table 5-27, Column D) × 49.55% × 5.00%	c (Table 5-27, Column D) × 49.55% × 95.00%	d (Table 5-27, Column E – Column D) × 50.45%	e (Table 5-27, Column D × 50.45%
1	300.28	-	-	305.77	-
2	41.05	-	-	41.80	-
3	41.05	-	-	41.80	-
4	41.05	-	-	41.80	-
5	41.05	-	-	41.80	-
6	41.05	7.20	136.79	41.80	146.62
7	41.05	0.98	18.70	41.80	20.05
8	41.05	0.98	18.70	41.80	20.05
9	41.05	0.98	18.70	41.80	20.05
10	41.05	0.98	18.70	41.80	20.05
Total	**670**	**11**	**212**	**682**	**227**

Note: Totals may not add due to rounding. Values rounded to hundredth decimal place unless otherwise displayed.

In Table 5-29, TSA calculates the total ten-year STA cost for cybersecurity coordinators, physical security coordinators, and accountable executives in the pipeline industry under

Alternative 3 by multiplying the number of STAs presented in Table 5-28 by the STA unit costs presented in Table 5-17.

Table 5-29: STA Costs for Cybersecurity Coordinators, Physical Security Coordinators, and Accountable Executives in the Pipeline Industry Under Alternative 3 ($ Thousands)

Year	In-Person Initial STA Cost	In-Person Renewal STA Cost	Online Renewal STA Cost	Initial Comparable STA Cost	Renewal Comparable STA Cost	Total STA Cost
	a (Table 5-28, Column A) × $352.67	b (Table 5-28, Column B) × $268.35	c (Table 5-22, Column C) × $63.41	d (Table 5-28, Column D) × $54.81	e (Table 5-28, Column E) × $42.41	f = ∑a,b,c,d,e
1	$105.9	-	-	$16.8	-	$122.7
2	$14.5	-	-	$2.3	-	$16.8
3	$14.5	-	-	$2.3	-	$16.8
4	$14.5	-	-	$2.3	-	$16.8
5	$14.5	-	-	$2.3	-	$16.8
6	$14.5	$1.9	$8.7	$2.3	$6.2	$33.6
7	$14.5	$0.3	$1.2	$2.3	$0.9	$19.1
8	$14.5	$0.3	$1.2	$2.3	$0.9	$19.1
9	$14.5	$0.3	$1.2	$2.3	$0.9	$19.1
10	$14.5	$0.3	$1.2	$2.3	$0.9	$19.1
Total	**$236.2**	**$3.0**	**$13.4**	**$37.4**	**$9.6**	**$299.6**

Note: Totals may not add due to rounding.

Lastly, in Table 5-30, TSA sums the STA costs for frontline employees and STA costs for cybersecurity coordinators, physical security coordinators, and accountable executives to calculate a total STA cost for the pipeline industry.

Table 5-30: Total STA Cost for Pipeline Industry ($ Thousands)

Year	Total STA Cost for Frontline Employees	Total STA Cost for Coordinators, and Accountable Executives	Total STA Cost
	a	b	c = ∑a,b
1	$6,389.0	$122.7	$6,511.6
2	$913.0	$16.8	$929.7
3	$918.6	$16.8	$935.4
4	$924.3	$16.8	$941.1
5	$930.1	$16.8	$946.8
6	$1,782.5	$33.6	$1,816.0
7	$1,062.6	$19.1	$1,081.7
8	$1,069.2	$19.1	$1,088.3
9	$1,075.8	$19.1	$1,094.9
10	$1,082.5	$19.1	$1,101.6
Total	**$16,147.6**	**$299.6**	**$16,447.2**

Note: Totals may not add due to rounding.

5.3.3.4 Total Cost of Alternative 3

In this section, TSA first presents the total STA cost for all modes followed by the total cost of Alternative 3, inclusive of the requirements outlined in the proposed rule.

In Table 5-31, TSA sums the ten-year STA costs for frontline employees in the pipeline industry; physical security coordinators in the pipeline industry; and cybersecurity coordinators as well as accountable executives for all modes covered under this alternative. The Cybersecurity coordinators and alternates, accountable executives, and physical security coordinators represent 2.6 percent of vetting costs for alternative 3 ($434,935) and pipeline frontline employees represent 97.4 percent of vetting costs for alternative 3 ($16,147,607).[443]

Table 5-31: Total STA Cost for All Modes ($ Thousands)

Year	Total STA Cost for Freight Rail	Total STA Cost for PTPR	Total Cost for Pipelines	Total STA Cost d = ∑a,b,c		
	a (Table 5-20)	b (Table 5-23)	c (Table 5-30)	Undiscounted	Discounted at 3%	Discounted at 7%
1	$44.3	$21.6	$6,511.6	$6,577.5	$6,386.0	$6,147.2
2	$2.1	$3.3	$929.7	$935.2	$881.5	$816.8
3	$2.2	$3.3	$935.4	$940.9	$861.1	$768.1
4	$2.2	$3.4	$941.1	$946.7	$841.1	$722.2
5	$2.2	$3.5	$946.8	$952.5	$821.7	$679.1
6	$12.6	$6.6	$1,816.0	$1,835.2	$1,536.9	$1,222.9
7	$2.7	$4.1	$1,081.7	$1,088.5	$885.1	$677.9
8	$2.8	$4.2	$1,088.3	$1,095.2	$864.6	$637.4
9	$2.8	$4.3	$1,094.9	$1,102.0	$844.6	$599.4
10	$2.8	$4.4	$1,101.6	$1,108.8	$825.0	$563.6
Total	**$76.7**	**$58.6**	**$16,447.2**	**$16,582.5**	**$14,747.5**	**$12,834.7**
Annualized					**$1,728.9**	**$1,827.4**

Note: Totals may not add due to rounding.

Next, TSA presents the cost of Alternative 3 which includes all costs of the proposed rule (across

[443] $76,711 (Column f, Table 5-20) + $58,633 (Column f, Table 5-23) + $299,591 (Column b, Table 5-30) = $434,935. (($16,582.5 (Column d, Table 5-31) × 1000) - $434,935)/ ($16,582.5 × 1000) = 0.974. Totals may not add due to rounding.

all modes and TSA) plus the additional cost for freight rail, PTPR, and pipeline industries.[444] Table 5-32 presents the total cost of the alternative, over the ten-year period of analysis, which equates to $3,106.4 million undiscounted, $2,645.7 million discounted at 3 percent and $2,174.4 million discounted at 7 percent. This alternative is $16.6 million more than the proposed rule undiscounted and $12.8 million more discounted at 7 percent.

[444] TSA expects the total cost OTRB under Alternative 3 to be the same as under the proposed rule, as OTRB owner/operators are not required to have cybersecurity coordinators or accountable executives who would undergo vetting.

Table 5-32: Total Cost to Industry and TSA Under Alternative 3 ($ Thousands)

Year	Industry				Total Cost to Regulated Industries	TSA	Total Cost		
	Pipelines	Freight Rail	PTPR	OTRB			g = ∑e,f		
	a	b	c	d	e = ∑a,b,c,d	f	Undiscounted	Discounted at 3%	Discounted at 7%
1	$92,147.8	$97,696.3	$120,017.9	$188.5	$310,050.6	$4,426.4	$314,477.0	$305,317.5	$293,903.8
2	$82,052.0	$95,473.5	$120,636.6	$6.0	$298,168.0	$2,407.7	$300,575.7	$283,321.4	$262,534.5
3	$80,067.4	$94,624.6	$121,511.2	$6.1	$296,209.3	$2,412.2	$298,621.5	$273,281.0	$243,764.1
4	$83,173.5	$97,004.9	$123,886.2	$6.3	$304,071.0	$1,358.2	$305,429.2	$271,369.9	$233,010.5
5	$81,211.9	$96,189.6	$124,817.4	$6.4	$302,225.3	$1,363.0	$303,588.3	$261,878.0	$216,454.3
6	$85,324.6	$98,687.6	$127,295.3	$6.6	$311,314.2	$1,367.6	$312,681.8	$261,866.1	$208,353.1
7	$82,646.6	$97,888.0	$128,283.5	$6.8	$308,824.8	$1,372.3	$310,197.2	$252,218.7	$193,175.2
8	$85,921.1	$100,407.9	$130,824.8	$6.9	$317,160.7	$1,377.2	$318,537.9	$251,456.7	$185,391.9
9	$84,008.8	$99,650.5	$131,878.1	$7.1	$315,544.5	$1,382.0	$316,926.5	$242,897.8	$172,387.0
10	$87,308.6	$102,203.3	$134,488.4	$7.3	$324,007.6	$1,387.1	$325,394.7	$242,124.2	$165,414.2
Total	**$843,862.3**	**$979,826.3**	**$1,263,639.4**	**$247.9**	**$3,087,575.9**	**$18,853.8**	**$3,106,429.8**	**$2,645,731.2**	**$2,174,388.5**
Annualized								**$310,160.4**	**$309,584.0**

Note: Totals may not add due to rounding.

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. The benefits associated with alternative 3 would include an increase in security to surface transportation through reduced potential security threats from compromised individuals handling sensitive information or operations. 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.

5.4 Summary of Alternatives

Table 5-33 presents the costs for the proposed rule and the three alternatives. TSA believes the proposed rule aligns with the agency's commitment to risk-based security policy and outcomes-based regulation; however, TSA presents these alternatives for public comment as potential options. In this section, TSA discusses in detail the arguments in favor of the proposed rule in comparison with each of the three alternatives.

Table 5-33: Comparison of Costs between Proposed Rule and Alternatives (Discounted at 7%, $ Thousands)

Regulatory Action	Initial Affected Population (Number of Owner/ Operators)	Description	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	(1) Freight Rail, PTPR, and Pipeline owner/operators are required to designate a cybersecurity coordinator; (2) report cybersecurity incidents; (3) have a cybersecurity risk management program approved by TSA; (4) retain employee training records; (5) be subject to inspections by TSA; (6) pipeline owner/operators must also designate a physical security coordinator and report physical security incidents to TSA; and (7) OTRB owner/operators are required to report cybersecurity incidents to CISA.	$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	Eliminates some requirements from proposed rule but retains (1) Governance of the CRM Program; (2) Designate Cybersecurity Coordinators; (3) Identification of Critical Cybersecurity Systems; (4) Reporting Cybersecurity Incidents; and (5) Cybersecurity Incident Response Plan	$76,963	$2,391	$79,354	$10,958	$340	$11,298
Alternative 2	Freight Rail – 6 PTPR – 27 OTRB – 71 Pipeline – 100	(1) Includes all requirements of the proposed rule; and (2) limits applicability to only Class I freight railroads, PTPR owner/operators that host Class I freight railroads or have an average daily ridership of 100,000 passengers, and the 100 most critical owner/operator of hazardous liquid and natural gas pipelines and liquefied natural gas facilities.	$1,589,258	$11,085	$1,600,343	$226,275	$1,578	$227,853
Alternative 3	Freight Rail – 73 PTPR – 34 OTRB – 71 Pipeline – 115	(1) Includes all requirements of the proposed rule and (2) introduces vetting for select employees in Freight Rail, PTPR, and Pipeline industries.	$2,160,147	$14,241	$2,174,388	$307,556	$2,028	$309,584

TSA has not selected any of the proposed alternatives and proposes this rule because TSA believes the proposed rule's requirements are the most likely to balance costs and benefits in the regulated industries from the harmful effects of cybersecurity incidents.

TSA considered Alternative 1, which scales back the requirements to only those minimally necessary to prevent the worst consequences of a cyber-incident, as insufficient. The alternative would provide TSA oversight at a reactionary level, but not include the visibility or accountability of any preventative efforts owner/operators are undertaking as many of the provisions relate to incident reporting and response as opposed to prevention efforts such as evaluation, planning, and implementation. Given the key role these industries play in the supply chain, movement of people and goods, and the economy as a whole and the dynamic and emerging cybersecurity threats to the nation's rail and hazardous liquid and natural gas pipeline infrastructure, TSA believes a more proactive approach toward reducing risk related to cybersecurity is necessary.

TSA considered Alternative 2, which keeps the requirements in scope from the preferred alternative, but narrows the applicability criteria. While this alternative represents a cost savings relative to the preferred alternative, TSA has not selected this alternative because it does not cover many owner/operators who play a critical role in contributing to the stability and security of the movement of people and goods. A successful incident on the owner/operators excluded from the applicability criteria in Alternative 2 may still have a large ripple effect throughout the economy.

TSA considered Alternative 3, which retains all requirements from the proposed rule and introduces a vetting requirement for select employees in the freight rail, PTPR, and pipeline

industries. TSA did not select this alternative because the primary objective of this rulemaking is to secure cyber-related surface transportation infrastructure. Moreover, TSA 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.

6 INITIAL REGULATORY FLEXIBILITY ANALYSIS

6.1 Summary of Findings

The Transportation Security Administration (TSA) has performed an Initial Regulatory Flexibility Analysis (IRFA) of the impacts on small businesses and other entities in the freight rail, public transportation and passenger rail (PTPR), over-the-road bus (OTRB), and pipeline owner/operators covered by this proposed rule. In this section, TSA describes the impact on covered entities separately, as the entities in each category tend to operate in different industries according to the North American Industry Classification System (NAICS).[445] TSA performed the IRFA using the assumptions and costs discussed in Sections 2 and 3 of this Regulatory Impact Analysis (RIA).

Based on the IRFA, TSA finds:

- An estimated 293 entities (i.e., 73 corporate-level freight railroads; 34 PTPR agencies; 71 OTRB owner/operators; and 115 pipeline owner/operators) would initially be affected by this proposed rule.[446] These entities include businesses and governmental jurisdictions. TSA did not find any non-profit organizations affected by this proposed rule.

- Based on an analysis of these 293 entities, TSA estimates that 79 (27 percent) are small entities. More specifically, TSA estimates that 17 freight railroads (23 percent of the 73 freight impacted population), 0 PTPR agencies (0 percent of the 34 PTPR impacted

[445] A majority of Class I, II, and III freight railroads analyzed fall into the Rail Transportation industry (NAICS 482), whereas a majority of the pipeline entities fall into Pipeline Transportation (NAICS 486) and Utilities (NAICS 221) industries. All of the PTPR entities, and a majority of the OTRB entities, fall within the Transit and Ground Transportation industry (NAICS 485).

[446] See Section 2.1 for a detailed discussion on the initial number of regulated freight rail entities, PTPR agencies, OTRB owner/operators, and pipeline owner/operators.

population), 55 OTRB owner/operators (78 percent of the 71 OTRB impacted population), and 7 pipeline owner/operators (6 percent of the 115 pipeline impacted population) are considered small entities.

- Regulated entities have different requirements under the proposed rule, depending on their industry. Freight railroad, PTPR, and Pipeline owner/operators would be required to designate a cybersecurity coordinator, report cybersecurity incidents, and have a Cybersecurity Risk Management (CRM) program approved by TSA, as well as familiarization, compliance, and recordkeeping requirements. Pipeline owner/operators have additional requirements to designate a physical security coordinator and report physical security incidents to TSA. OTRB owner/operators only have to 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 entities, $682 per entity for OTRB entities, and $484,848 per entity for pipeline entities,[447] and $537 per employee for freight rail entities and $659 per employee for pipeline entities[448] in the highest cost year of the proposed rule.[449]

- TSA estimates the proposed rule would have an impact greater than 1 percent of annual revenue on 11 small freight rail entities.

---

[447] This includes employer-paid cost of employee time, such as cybersecurity training for employees. TSA assumes all requirements performed by employees occur while they are on duty, therefore all employee costs are borne by the entity.

[448] The per employee costs provided in this analysis are for freight rail and pipeline owner/operators only, since none of the in-scope PTPR owner/operators are small and there are no per employee costs for OTRB owner/operators in the proposed rule.

[449] Year 10 is the highest cost year of the proposed rule for freight rail, PTPR, and pipeline entities, and Year 1 is the highest cost year for OTRB entities (see Table 3-95).

6.2 Overview of the IRFA

The Regulatory Flexibility Act (RFA) establishes "as a principle of regulatory issuance that agencies shall endeavor, consistent with the objectives of the rule and of applicable statutes, to fit regulatory and informational requirements to the scale of the businesses, organizations, and governmental jurisdictions subject to regulation. To achieve this principle, agencies are required to solicit and consider flexible regulatory proposals and to explain the rationale for their actions to assure that such proposals are given serious consideration."[450]

The RFA at 5 U.S.C. 603 requires agencies to prepare a regulatory flexibility analysis that examines the impacts of a proposed rule on small entities. Section 605 of the RFA allows an agency to certify a rule in lieu of preparing an analysis if the regulation is not expected to have a significant economic impact on a substantial number of small entities.

In accordance with the RFA, TSA has prepared an IRFA that examines the impacts of the proposed rule on small entities (5 U.S.C. 601 et seq). The RFA covers a wide range of small entities. The term "small entities" comprises small businesses, not-for-profit organizations that are independently owned and operated and are not dominant in their fields, and governmental jurisdictions with populations of less than 50,000. 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 SBA definition for a small business or establish an alternative definition for the industry. TSA uses the SBA small business size standards for each relevant industry.

[450] 5 U.S.C. 601 note.

The small businesses and small governmental jurisdictions affected by the proposed rule include freight railroad owner/operators, OTRB owner/operators, and Pipeline owner/operators. TSA used available operator/owner name and address information to research public and proprietary databases for the entity type (subsidiary or parent company), primary line of business, employee size, revenue, and other information. These databases include Data Axle Reference Solutions[451] and Dun & Bradstreet.[452] TSA matched this information to the thresholds in the SBA "Table of Small Business Size Standards" to determine if an entity is small in its primary line of business as classified in NAICS.[453] In addition, for small governmental jurisdictions, TSA pulled collected U.S. Census Bureau data on jurisdiction size.[454]

This IRFA contains the following:

- A description of the reasons why action by the agency is being considered;
- A succinct statement of the objectives of, and legal basis for, the proposed rule;
- A description of and, where feasible, an estimate of the number of small entities to which the proposed rule would apply;
- A description of the projected reporting, recordkeeping, and compliance requirements of the proposed rule, including an estimate of the classes of small entities which would be subject to the requirements and the type of professional skills necessary for preparation of

[451] Data Axle Reference Solutions (https://www.data-axle.com).
[452] D&B Finance Analytics. Dun & Bradstreet. https://financeanalytics.dnb.com/.
[453] SBA. Table of Small Business Size Standards Matched to North American Industry Classification System Codes. https://www.sba.gov/sites/default/files/files/Size_Standards_Table_2022.pdf. Effective May 2, 2022. Retrieved August 22, 2022.
[454] U.S. Census Bureau. Population and Housing Unit Estimates Datasets. https://www.census.gov/programs-surveys/popest/data/data-sets.html. Accessed January 24, 2023.

the report or record;

- An identification, to the extent practicable, of all relevant Federal rules that may duplicate, overlap, or conflict with the proposed rule; and

- A description of any significant alternatives to the proposed rule that accomplish the stated objectives of applicable statutes and may minimize any significant economic impact of the proposed rule on small entities, including alternatives considered.

Although TSA broadly addresses the aforementioned item in this section, TSA does refer the reader to the applicable sections of the RIA where more detail is available. TSA also includes a discussion of the sensitivity analysis TSA performed and its comparative impact on small entities. TSA is publishing this IRFA to aid the public in commenting on the potential small entity impacts of the requirements in this proposed rule. 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 this proposed rule. TSA will consider all information and comments received in the public comment process when making a determination regarding the economic impact on small entities in the final rule.

6.3 A Description of the Reasons Why Action by the Agency Is Being Considered

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 counterterrorism mission assigned to TSA. Surface transportation systems in particular—including public transportation systems, intercity and commuter passenger railroads, freight railroads, intercity buses, pipelines, and related

infrastructure—are vital to our economy and essential to national security.[455] TSA is proposing to impose requirements on freight rail, PTPR, and pipelines that would mandate a cybersecurity risk management (CRM) program. Cybersecurity has a growing impact on the economy and potential risks to national security and public safety. This proposed rule helps address current and emerging cybersecurity threats to entities involved in the transportation of passengers and commodities by rail, OTRB, and/or pipelines. Executive Order 13636 (Improving Critical Infrastructure Cybersecurity)[456] recognized the Federal Government's efforts to secure our Nation's critical infrastructure, which includes transportation systems.

To defend against malicious cyber-related activities, Executive Order 13694 (Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities)[457] recognized malicious cyber-related activities as an "extraordinary threat to the national security, foreign policy, and economy of the United States," warranting a national emergency.[458] The National Emergency with Respect to Significant Malicious Cyber-Enabled Activities has been extended as of March 30, 2022.[459] Executive Order 14028 (Improving the Nation's Cybersecurity)[460] also recognized that "the private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with

---

[455] Surface Transportation and Rail Security Act of 2007, report of the Senate Committee on Commerce, Science, and Transportation at 2 (S Rpt. 110-29, dated March 1, 2007) quoting EO 13416 (Dec. 5, 2006), published at 71 FR 71033 (Dec. 7, 2006). https://www.govinfo.gov/content/pkg/CRPT-110srpt29/html/CRPT-110srpt29.htm.

[456] Executive Order 13636: Improving Critical Infrastructure Cybersecurity. Feb. 12, 2013. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[457] Executive Order 13694: Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities. Apr. 1, 2015. https://www.federalregister.gov/documents/2015/04/02/2015-07788/blocking-the-property-of-certain-persons-engaging-in-significant-malicious-cyber-enabled-activities,

[458] 80 FR 18077, April 2, 2015.

[459] 87 FR 18963, March 31, 2022.

[460] Executive Order 14028: Improving the Nation's Cybersecurity. May 12, 2021. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/,

the Federal Government to foster a more secure cyberspace."[461]

In 2021, the President issued the "National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems,"[462] which CISA, in coordination with the National Institute of Standards and Technology (NIST), to develop baseline voluntary Cybersecurity Performance Goals (CPGs) that could be used consistently across all critical infrastructure sectors.

6.4 A Succinct Statement of the Objectives of, and Legal Basis for, the Proposed Rule

The Aviation and Transportation Security Act, Pub. L. 107-71, 115 Stat. 597 (November 19, 2001), gives TSA broad responsibility and authority for "security in all modes of transportation" including aviation and "other modes of transportation that are exercised by the Department of Transportation." *See* 49 U.S.C. 114(d). In addition, as part of the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Act), Congress enacted requirements related to protection of certain critical pipelines, freight rail carriers, and public transit passenger railroad (PTPR) entities. This proposed rule is consistent with TSA's mission, as well as TSA's responsibility and authority identified above.

TSA, under this authority, can establish regulations to enhance the cybersecurity posture of regulated entities. TSA, following input from CISA, Department of Transportation (including the Federal Railroad Administration, Pipeline and Hazardous Materials Safety Administration, and the Federal Transit Administration), the Federal Energy Regulatory Commission (FERC), the

---

[461] 86 FR 26633, May 17, 2021.
[462] The White House. Jul. 28, 2021. National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems.www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/.

Department of Energy, the United States Coast Guard, and consultation with industry stakeholders proposes this rulemaking to enhance the cybersecurity posture of surface modes and meet aspects of its statutory obligations under the 9/11 Act. The required cybersecurity measures provide covered entities with an improved ability to prevent cyber-attacks, mitigate the damage from a cyber-attack, and more quickly recover from a cyber-attack. The benefits related to these outcomes are discussed in Section 4.

TSA is proposing to require all entities currently subject to TSA's regulatory requirements to report security incidents to TSA to also report cybersecurity incidents to CISA. Designated freight railroads, public transportation agencies, rail transit systems, and pipeline systems and facilities would also be required to have a CRM program approved by TSA.

The proposed CRM program includes three primary elements. First, owner/operators within the applicability would be required to regularly 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 Cybersecurity Framework. Second, owner/operators would be required to develop a Cybersecurity Operational Implementation Plan (COIP) that includes the following information: (a) identification of individuals/positions responsible for the governance of the owner/operators CRM program; (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 and monitor these Critical Cyber Systems; and (e) measures to address response and recovery to a cybersecurity incident. While many of these measures for the COIP are limited to Critical Cyber Systems, all owner/operators within the applicability would

be required to have a CIRP. Third, owner/operators would be required to have a Cybersecurity Assessment Plan that includes an independent evaluation of the effectiveness of their CRM program and identification of unaddressed vulnerabilities.

6.5 A Description of and, Where Feasible, an Estimate of the Number of Small Entities to Which the Proposed Rule Would Apply

Small businesses, organizations, and governmental jurisdictions are collectively referred to as small entities for purposes of the IRFA. TSA used the names and addresses of sampled freight railroads, PTPR agencies, OTRB owner/operators, and pipeline owner/operators to search for the entities' NAICS codes, annual revenues, and number of employees using various databases. Average annual receipts[463] and the average annual number of employees per business are the two primary indicators by which the SBA classifies businesses as small for each NAICS code. In addition, TSA used jurisdiction size, based on U.S. Census Bureau data, as the primary indicator to classify governmental jurisdictions as small. TSA notes that the performance-based structure of the rule provides accommodation for small businesses. Owner/operators would develop plans as appropriate for their size and operations. For instance, while a large company may have thousands of systems, a smaller company may have a dozen. A larger company may have a centralized badging system compared to a smaller company that relies on a program that regularly changes passwords when an employee's privilege changes (the employee departs or changes responsibilities).

[463] As defined in 13 CFR § 121.104(a), receipts are all revenue in whatever form received or accrued from whatever source, including from the sales of products or services, interest, dividends, rents, royalties, fees, or commissions, reduced by returns and allowances. Generally, receipts are considered "total income" (or in the case of a sole proprietorship "gross income") plus "cost of goods sold" as these terms are defined and reported on Internal Revenue Service (IRS) tax return forms.

6.5.1 Number of Small Freight Railroad Entities Regulated Under the Proposed Rule

As described in Sect 2.1.1, TSA determined that for freight railroads, the covered population includes the following:

- Is a Class I railroad as defined in current 49 CFR 1580.3; or
- Is a Class II or III railroads that:
  - Transports one or more of the categories and quantities of Rail Security-Sensitive Materials in a High Threat Urban Area;
  - 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 years before the effective date of the final rule or in any calendar year after the effective date;
  - Is designated as a Defense Connector Railroad by DoD; 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.

TSA identified 73 freight rail owner/operators covered by the proposed rule. This includes six Class I, and 67 Class II or Class III freight rail owner/operators. Where possible, TSA obtained NAICS codes, employee size, and revenue data using Data Axle Resource Solutions and Dun & Bradstreet. Using the reported NAICS codes, TSA determined that the freight railroads operate in 14 different industries. A majority of the freight rail owner/operators, 80 percent, operate in the Line Haul Railroads industry (NAICS 482111). The remaining 20 percent of freight rail owner/operators operate in 13 different industries with no other NAICS code covering more than two freight rail owner/operators. The SBA small business threshold is 1,500 employees for Line

Haul Railroads, with other industries having various other criteria.

Of the 73 freight rail owner/operators, TSA found revenue and employment size data with at least one NAICS code on 69 freight rail owner/operators in Data Axle Reference Solutions. The four entities not found in Data Axle Reference Solutions were then checked through Dun & Bradstreet. Of the 73 freight rail owner/operators, there are seven entities owned or operated by a government entity with a jurisdictional population of greater than 50,000, therefore are not considered small. TSA identified 17 freight rail owner/operators that are considered small by the SBA size standard, representing 23 percent of the freight rail owner/operators regulated under the proposed rule. Table 6-1 shows the breakdown of freight railroad entities by NAICS code.

Table 6-1: Number of Small Businesses Affected by the Proposed Rules' Requirements for Freight Rail Owner/Operators

NAICS Code	NAICS Industry Description	SBA Size Standard	Count of Owner/Operators	Count of Small Entities
482111	Line Haul Railroads	1,500 Employees	58	17
324110	Petroleum Refineries	1,500 Employees	2	0
523910	Miscellaneous Intermediation	$47,000,000 in Receipts	2	0
212290	Natural Gas Distribution	1,000 Employees	1	0
237210	Land Subdivision	$34,000,000 in Receipts	1	0
237990	Dredging and Surface Cleanup Activities	$45,000,000 in Receipts	1	0
484121	General Freight Trucking, Long Distance, Truckload	$34,000,000 in Receipts	1	0
488210	Support Activities for Rail Transportation	$34,000,000 in Receipts	1	0
488310	Port and Harbor Operations	$47,000,000 in Receipts	1	0
488510	Freight Transportation Arrangement	$20,000,000 in Receipts	1	0
541614	Process, Physical Distribution and Logistics Consulting Services	$20,000,000 in Receipts	1	0
551112	Offices of Other Holding Companies	$45,500,000 in Receipts	1	0
561520	Tour Operators	$25,000,000 in Receipts	1	0
921120	Public Administration	N/A	1	0
Total			**73**	**17**

6.5.2 Total Cost Per Small Freight Railroad Owner/Operators Affected

TSA measured the impact of the proposed rule on these small freight railroad entities by estimating the unit cost of the requirements that would result in costs for small entities: designate

a cybersecurity coordinator and alternate; report cybersecurity incidents to CISA; establish a CRM program; familiarization; compliance; and recordkeeping. Since entities would incur the highest cost in the tenth year of the analysis, as described in Section 3.6, TSA focuses on the Year 10 costs for this IRFA. TSA understands many of the requirements in the proposed rule may already be performed by covered entities; however, the costs calculations assume none of the covered entities are currently performing the requirements of the rule, as discussed in Section 1.7. TSA used the burden hours discussed in Section 2 to account for the opportunity costs of performing each requirement.[464] TSA combined these burden hours with fully-loaded compensation rates of a corporate security manager ($85.93 per hour),[465] cybersecurity coordinator ($127.70 per hour)[466], cybersecurity analyst ($67.34 per hour)[467], network and computer systems administrator ($64.63 per hour),[468] freight rail cybersecurity employee ($97.28 per hour),[469] freight rail all occupations ($53.19),[470] audit manager ($92.65 per hour),[471] administrative assistant ($40.42 per hour),[472] attorney ($130.21 per hour),[473]and Chief Executive ($202.60).[474] TSA calculated costs by using the loaded compensation rates of each occupation involved in meeting a requirement, and blending them based on the proportion of the requirement attributed to that job title.

---

[464] The requirement to establish a CRM program has multiple sub requirements, such as familiarization, evaluation, review and compliance, cybersecurity training, recordkeeping, etc. The entire list of requirements, including sub requirements, is displayed in Table 7.3.
[465] Hourly compensation rate estimated based on BLS data and adjusted by industry composition. See Section 2.3.1.
[466] *Ibid.*
[467] *Ibid.*
[468] *Ibid.*
[469] *Ibid.*
[470] *Ibid.*
[471] *Ibid.*
[472] *Ibid.*
[473] *Ibid.*
[474] *Ibid.*

TSA estimates a training, training recordkeeping, and access control equipment under the CRM Program cost on a per-employee basis, based on the burden assumptions described in Sections 3.1.3.5 and 3.1.3.6. TSA estimates the average cost per employee is $536.55, and the average small freight rail entity has 97 employees.[475]

TSA estimates cybersecurity coordinator, cybersecurity incident reporting, and all other CRM Program costs, familiarization, compliance, and compliance recordkeeping costs on a per-entity basis based on burden assumptions described in Sections 3.1.1 to 3.1.8. However, TSA recognizes these costs may vary by individual owner/operator based on choices made under the proposed rule performance standards and the size of their operations. Though not quantified, such variance may include lower costs by not requiring as extensive of plans or backup systems as well as potential increased costs associated with hiring out activities that cannot be performed in house.

TSA then added each small freight railroad's total employee costs[476] to the per entity cost of $486,792 to estimate the total cost per small freight railroad of $536,817 in Year 10. Table 6-2 displays the costs of each of the proposed requirements for small freight rail owner/operators.

[475] TSA obtained employment information on all 17 small freight railroad owner/operators, which totaled 1,648. Therefore, the average number of employees is 1,648 ÷ 25 = 96.96 per owner/operator.
[476] $536.55 × 96.96 employees/entity = $52,023.89.

Table 6-2: Total Cost per Small Freight Rail Owner/Operator

Requirement	Unit Time (hours)	Hourly Wage Rate	Unit Cost
	a	b	c = b x a
Cybersecurity Training	1.30	$63.36	$82.37
Cybersecurity Training Recordkeeping	0.02	$40.42	$0.81
CRM Program (Access Control Software & Hardware)	7.17	$53.19	$453.37[477]
Costs per Employee			**$536.55**
Familiarization	14.66	$129.88	$1,904.04
Cybersecurity Incident Reporting	0.14	$97.22	$13.61
CRM Program	3,030.17	$74.24	$224,959.00
CIRP	300.00	$94.36	$28,307.60
Other Costs[478]	-	-	$231,607.91
Cost per Entity			**$486,792.16**

Note: Totals may not add due to rounding.

6.5.3 Cost Impact on Small Freight Railroads as Percentage of Revenue

TSA divides the estimated cost in Year 10 by the reported annual revenue for each of the 17 small freight railroad entities to measure the impact the proposed rule would have on annual revenue. Table 6-3 presents the number and percentage of small freight railroad entities categorized by the percentage of tenth-year costs compared to annual revenues.

Table 6-3: Cost Impact on Small Freight Railroads as Percentage of Revenue

Revenue Impact Range	Number of Affected Small Entities	Percentage of Affected Small Entities
0% < Impact ≤ 1%	6	35%
1% < Impact ≤ 3%	3	18%
3% < Impact ≤ 5%	4	24%
5% < Impact ≤ 10%	2	12%
Above 10%	2	12%
Total	**17**	**100%**

Note: Totals may not add due to rounding.

TSA estimates that 11 small entities, or 65 percent of the 17 small freight entities covered by the proposed rule, would have an impact greater than one percent of revenue, with four entities having an impact over 5 percent of revenue including two over 10 percent. The entities with greater impact include Class III railroads with less than 40 employees each, but interchange with

[477] Includes additional $72 per employee cost for MFA equipment.

[478] Other costs include data backup, system monitoring, and other costs not based on unit time × hourly wage rate.

two or more Class I railroads and therefore are subject to the proposed rule's requirements. Applicability of the proposed rule is tied to potential impacts and entities are expected to meet the same security standards; however, as stated previously, actual impacts may be less than estimated based on the scale of an entity's operation.

TSA welcomes comments from the public on ways to mitigate the cost impacts of the proposed rule on small entities, while meeting cybersecurity goals within the freight rail industry.

6.5.4 Number of Small PTPR Owner/Operators Regulated Under the Proposed Rule

As described in Section 2.1.2, TSA determined that for PTPR owner/operators, the covered population should include the following:

- Amtrak (also known as the National Railroad Passenger corporation) or 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 railroads that hosts a Class I railroad or Amtrak, regardless of ridership volume; or
- 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.

The criteria cover PTPR agencies that are responsible for transporting more than 90 percent of the total nationwide daily ridership volume. TSA identified 34 PTPR entities that would be covered by the proposed rule. All PTPR agencies are listed in Data Axle Reference Solutions with the NAICS code of 485112 (Commuter Rail Systems). Of the 34 PTPR agencies, 33 are owned or operated by government jurisdictions with populations greater than 50,000 and are

therefore not considered to be small entities. For the remaining PTPR agency, the annual revenue exceeds the SBA size standards for their NAICS code.[479] Table 6-4 depicts the number of small PTPR owner/operators affected by the proposed requirements.

Table 6-4: Number of Small PTPR Owner/Operators Affected by the Proposed Rule's Requirements for PTPR Owner/Operators

NAICS Code	NAICS Industry Description	SBA Size Standard	Count of Owner/Operators	Count of Small Entities
485112	Commuter Rail Systems	$47,000,000 in Receipts	1	0
N/A	Government	50,000 Population	33	0
Total			**34**	**0**

6.5.5 Number of Small OTRB Owner/Operators Regulated Under the Proposed Rule

As described in Section 2.1.3, Section § 1584.107 details the criteria for inclusion or applicability of the proposed rule for over-the-road-buses (OTRBs). Where possible, TSA obtained NAICS codes, employee size, and revenue data for this population using Data Axle Resource Solutions and Dun & Bradstreet.

TSA identified 71 OTRB owner/operators covered by the proposed rule. Of these, TSA found revenue and employment size data with at least one NAICS code on 63 entities in Data Axle Reference Solutions. The remaining eight entities were then checked with Dun & Bradstreet, and employee and revenue data was found on four of them. The four entities where employment and revenue data was not found are considered small for the purposes of this analysis. Of the 71 OTRB owner/operators identified, 55 (77.5 percent) are small or assumed to be small. This information is displayed in Table 6-5.

[479] 33 of the 34 PTPR entities covered by the proposed rule are owned or operated by government jurisdictions with populations greater than 50,000. The entity that is owned or operated as a private company has annual revenue exceeding the SBA Size Standard for NAICS 485112 (Commuter Rail Systems) of $41.5 million.

Table 6-5: Number of Small Businesses Affected by the Proposed Rule's Requirements for OTRB Owner/Operators

NAICS Code	NAICS Industry Description	SBA Size Standard	Count of Owner/Operators	Count of Small Entities
485510	Charter Bus Industry	$19,000,000 in Receipts	21	18
485210	Interurban and Rural Bus Transportation	$32,000,000 in Receipts	17	8
561520	Tour Operators	$25,000,000 in Receipts	9	9
488210	Support Activities for Rail Transportation	$34,000,000 in Receipts	6	6
485999	All Other Transit and Ground Passenger Transportation	$19,000,000 in Receipts	5	4
485410	School and Employee Bus Transportation	$30,000,000 in Receipts	2	1
484230	Specialized Freight (except Used Goods) Trucking, Long Distance	$34,000,000 in Receipts	2	2
487210	Scenic and Sightseeing Transportation, Water	$14,000,000 in Receipts	1	1
523910	Miscellaneous Intermediation	$47,000,000 in Receipts	1	0
485320	Limousine Service	$19,000,000 in Receipts	1	1
532111	Passenger Car Rental	$47,000,000 in Receipts	1	0
483211	Inland Water Freight Transportation	1,500 Employees	1	1
N/A	No Data	N/A	4	4
Total			**71**	**55**

6.5.6 Total Cost Per Small OTRB Owner/Operator

TSA measured the impact of the proposed rule on small OTRB owner/operators by estimating the unit cost of the proposed requirements that would result in costs for small entities. The proposed rule would require OTRB operators to report cybersecurity incidents to CISA; however, TSA also included the cost to entities to familiarize themselves with this rule. There are no per employee costs to OTRB owner/operators in the proposed rule. Since OTRB entities incur the highest cost in the first year of the analysis, TSA focuses on the Year 1 costs for this IRFA.[480] TSA used the burden hours discussed in Sections 3.3.1 and 3.3.2 to account for familiarization with the rule and reporting cybersecurity incidents to CISA. TSA multiplies these

[480] OTRB is the only mode with highest cost year being Year 1; all other modes have highest costs in Year 10.

burden hours by the equivalent hourly compensation rate of an OTRB Cybersecurity Coordinator ($105.82 per hour), Cybersecurity Analyst ($63.15 per hour), and Audit Manager ($60.44 per hour), as discussed in Section 2.3.3, to generate a tenth-year cost estimate for small OTRB entities. The cost per small OTRB owner/operator are depicted in Table 6-6.

Table 6-6: Total Cost per Small OTRB Owner/Operator

Requirement	Unit(s) (Hours per Entity)	Cost per Hour[481]	Cost per Small Entity
	a	b	c = b × a
Familiarization Costs	8.00	$83.40	$667.20
Report Cybersecurity Incidents to CISA	0.18	$84.76	$15.14
Cost per Entity	**8.18**		**$682.34**

Note: Totals may not add due to rounding.

6.5.7 Cost Impact on Small OTRB Owner/Operators as Percentage of Revenue

TSA divides the estimated tenth-year cost by reported annual revenue for each of the 51 small OTRB owner/operators (that had full information available) to measure the impact that the proposed rule would have on annual revenue. None of the small OTRB entities had costs greater than 1% of annual revenue. Table 6-7 presents the number and percentage of small OTRB entities categorized by the percentage of Year 10 costs compared to annual revenues.

Table 6-7: Cost Impact on Small OTRB Owner/Operators as Percentage of Revenue

Revenue Impact Range	Number of Affected Small Entities[482]	Percentage of Affected Small Entities
0% < Impact ≤ 1%	47	100%
1% < Impact ≤ 3%	-	-
3% < Impact ≤ 5%	-	-
5% < Impact ≤ 10%	-	-
Above 10%	-	-
Total	**47**	**100%**

TSA estimates that the tenth-year cost of the proposed rule would have an impact of less than 1 percent of revenue for all 47 small OTRB entities.

[481] These are blended rates based on the amount of time TSA calculates an individual from each job title performs each requirement.
[482] The values in this table reflect only small OTRB entities with available revenue data.

6.5.8 Number of Small Pipeline Owner/Operators Regulated Under the Proposed Rule

As described in Section 2.1.4, pipeline owner/operators covered by the proposed rule include the following:

- Hazardous liquid pipelines that are subject to 49 CFR part 195 and—
  - Annually deliver 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
  - Are 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;[483]
- Operate a primary control room that is responsible for multiple systems 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; or
- Have a contract with the Defense Logistics Agency to supply hazardous liquids in excess of 70,000 barrels annually.[484]

For owner/operators of natural gas and other gas pipelines, the criteria and thresholds were developed by TSA specifically for this proposed rule. The criteria are similar to that used by TSA to identify critical pipeline operators, based on risk, as set forth in the statutory requirement

[483] *See* proposed 49 CFR part 1586 for a definition of High Consequence Area and a discussion of Terms in subsection D of this section.

[484] The criteria for 70,000 barrels is pending coordination with the Defense Logistics Agency. This amount conforms to what TSA uses to identify critical pipeline systems ("Top 100").

to identify the 100 most critical pipeline operators.[485] The proposed CRM program requirements includes each company that:

- The natural and other gas systems are subject to 49 CFR part 192 and—
  - 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;
  - Delivered natural or other gas to 275,000 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
  - For natural gas transmission, have in excess of 200 segment miles that could affect a High Consequence Area;
- Operate a primary control room responsible for multiple systems and the total annual delivery for those systems combined Is greater than 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; or
- Provide natural gas service to greater than 275,000 meters (or service points) annually (generally natural gas distribution or LDC) in any of the three calendar years before

[485] *See* 6 U.S.C. 1207(b).

the effective date of the final rule, or any single calendar year after the effective date of the final rule.

For owners/operators of Liquefied Natural Gas (LNG) facilities, the proposed CRM program apply to facilities that import LNG or that serve as peak shaving facilities.

TSA identified 115 Pipeline owner/operators covered by the proposed rule. Of these, TSA found revenue and employment size data with at least one NAICS code for 98 entities in Data Axle Reference Solutions. The 17 remaining pipeline entities that were not found in Data Axle Reference Solutions were checked against Dun & Bradstreet in which TSA found revenue and employment size data for the remaining entities.

Of the 115 entities TSA identified as covered by the proposed rule, 7 are small. Table 6-8 shows the breakdown of the small regulated pipeline entities by NAICS codes.

Table 6-8: Number of Small Pipeline Owner/Operators Affected by the Proposed Rule's Requirements

NAICS Code	NAICS Industry Description	SBA Size Standard	Count of Owner/Operators	Count of Small Entities
221200	Natural Gas Distribution	1,000 Employees	20	2
486100	Pipeline Transportation of Crude Oil	1,500 employees	17	5
221100	Electric Power Generation, Transmission and Distribution	1,000 Employees	17	0
486200	Pipeline Transportation of Natural Gas	$41,500,000 in Receipts	10	0
551112	Offices of Other Holding Companies	$45,500,000 in Receipts	8	0
211120	Natural Gas Extraction	250 employees	7	0
324110	Petroleum Refineries	1,500 employees	6	0
541618	Other Management Consulting Services	$19,000, 000 in Receipts	3	0
213112	Support Activities for Oil and Gas Operations	$47,000,000 in Receipts	2	0
325998	All Other Miscellaneous Chemical Product and Preparation Manufacturing	500 employees	2	0
238220	Plumbing, Heating, and Air Conditioning Contractors	$19,000,000 in Receipts	2	0
523910	Miscellaneous Intermediation	$47,000,000 in Receipts	2	0
236115	New Single-family Housing Construction (Except For- Sale Builders)	$45,000,000 in Receipts	1	0
424710	Petroleum Bulk Stations and Terminals	225 employees	1	0
486910	Pipeline Transportation of Refined Petroleum Products	1,500 employees	1	0
488490	Other Support Activities for Road Transportation	$18,000,000 in Receipts	1	0
493110	General Warehousing and Storage	$34,000,000 in Receipts	1	0
221118	Other Electric Power Generation	250 Employees	1	0
221310	Water Supply and Irrigation Systems	$41,000,000 in Receipts	1	0
523940	Portfolio Management and Investment Advice	$47,000,000 in Receipts	1	0
541810	Advertising Agencies	$25,500,000 in Receipts	1	0
237130	Power and Communication Line and Related Structures Construction	$45,000,000 in Receipts	1	0
541990	All Other Professional, Scientific and Technical Services	$19,500,000 in Receipts	1	0
541612	Human Resources Consulting Services	$29,000,000 in Receipts	1	0
999990	Unclassified Establishments	N/A	4	0
Total			115	7

6.5.9 Total Cost Per Small Pipeline Owner/Operators

The proposed rule would require corporate-level pipeline owner/operators to perform eight

requirements: designate a physical security coordinator and alternate; report physical security incidents to TSA; designate a cybersecurity coordinator and alternate; report cybersecurity incidents to CISA; establish a CRM program; familiarization; compliance; and recordkeeping. Since pipeline owner/operators would incur the highest cost in the tenth year of the analysis, TSA focuses on the Year 10 costs for this IRFA. TSA used the burden hours discussed in Section 2 and the assumptions discussed in Section 3.4 to account for performing these requirements. TSA combined these burden hours with the hourly compensation rates of a corporate physical security manager ($128.40), cybersecurity coordinator ($118.09), cybersecurity analyst ($71.00), network and computer systems administrator ($61.21), all pipeline cybersecurity-sensitive positions ($67.44), audit manager ($138.10), all pipeline employees ($69.32), administrative assistant ($40.63), attorney ($280.21), and Chief Executive ($267.30) as discussed in Section 2.3.4. TSA calculated costs by using the respective compensation rates and blending them based on the proportion of the requirement attributed to that job title.[486] Table 6-9 displays the costs of each of the proposed requirements for small pipelines.

[486] For example, if TSA believes a requirement will be done by a cybersecurity coordinator working with two cybersecurity analysts, each contributing 1 hour, the blended rate is the sum of one cybersecurity coordinator's loaded compensation rate ($127.51) and the two cybersecurity analyst compensation rates ($67.56 × 2). TSA then divides this by the total hour burden. $87.54 = ($127.51 + (2 × $67.56)) ÷ 3.

Table 6-9: Total Cost per Small Pipeline Owner/Operator

Requirement	Unit Time (hours)	Hourly Wage Rate	Unit Cost
	a	b	c = b x a
Cybersecurity Training	1.30	$68.89	$89.55
Cybersecurity Training Recordkeeping	0.02	$40.63	$0.81
CRM Program (Access Control Software & Hardware)	7.17	$69.32	$569.02
Costs per Employee			**$659.38**
Security Coordinator	1.00	$128.40	$128.40
Security Incident Reporting	1.26	$130.24	$164.69
Cybersecurity Incident Reporting	3.48	$94.55	$329.03
CRM Program	3,125.36	$72.20	$225,664.35
CIRP	300.00	$89.84	$26,953.40
Other Costs	N/A	N/A	$231,607.91
Cost per Entity			**$484,847.79**

Note: Totals may not add due to rounding.

6.5.10 Cost Impact on Small Pipeline Owner/Operators as a Percentage of Revenue

TSA obtained employee data for all of the 23 affected small pipelines. TSA then calculated the training, recordkeeping, and CRM Program costs per entity based on the multiplication of an average of the 7 small pipeline owner/operators average number of employees[487] by the per employee cost of $659. TSA then added each small pipeline's total employee costs[488] to the per entity cost of $484,848 to estimate the cost per small pipeline owner/operator of $613,810 in Year 10.

TSA divides the estimated tenth-year cost by reported annual revenue for each of the 7 small pipeline owner/operators that had revenue information available to measure the impact that the proposed rule would have on annual revenue. Table 6-10 presents the number and percentage of small pipeline entities categorized by the percentage of Year 10 costs compared to annual revenues.

[487] TSA calculated the average number of employees per small pipeline owner/operators to be 195.6.
[488] $447.95 × 195.6 = $128,962.61

Table 6-10: Cost Impact on Small Pipeline Owner/Operators as Percentage of Revenue

Revenue Impact Range	Number of Affected Small Entities	Percentage of Affected Small Entities
0% < Impact ≤ 1% 1% < Impact ≤ 3% 3% < Impact ≤ 5% 5% < Impact ≤ 10% Above 10%	7	100%
Total	**7**	**100%**

Note: Totals may not add due to rounding.

TSA estimates that the costs in Year 10 of the proposed rule would have an impact of less than 1 percent of revenue for all of the small pipeline owner/operators , or 100 percent.

6.5.11 Summary of Revenue Impact on Affected Small Entities

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 railroads, 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 of them.[489] Table 6-11 presents the number and percentage of small entities with employment and revenue data impacted by percentage of Year 10 costs compared to annual revenues. The IRFA finds that 11 of the analyzed entities (13.9 percent) would have an impact greater than 1 percent of their annual revenue. Within this group, 4 (5.1 percent) would have an impact greater than 5 percent and 2 (2.5) would have an impact greater than 10 percent.

[489] TSA was unable to find revenue or employee data on four OTRB entities, which are assumed to be small.

Table 6-11: Revenue Impact on Affected Small Entities, Total

Revenue Impact Range	Number of Affected Small Entities	Percentage of Affected Small Entities
0% < Impact ≤ 1%	68	86.1%
1% < Impact ≤ 3%	3	3.8%
3% < Impact ≤ 5%	4	5.1
5% < Impact ≤ 10%	2	2.5
Above 10%	2	2.5
Total	**79**	**100%**

Note: Totals may not add due to rounding.

TSA welcomes comments from small entities that may be impacted by the proposed rule, including additional costs or burdens not captured in this IRFA, and comments on methods to alleviate cost burdens to small entities while still reducing security and cybersecurity risk in their respective transportation modes.

6.6 A Description of the Projected Reporting, Record Keeping, and Other Compliance Requirements of the Proposed Rule, including an Estimate of the Classes of Small Entities That Would Be Subject to the Requirement and the Type of Professional Skills Necessary for Preparation of the Report or Record

Under the provisions of the proposed rule, the regulated populations would incur costs associated with reporting cybersecurity incidents to CISA for all covered entities. The other main requirements of the proposed rule require all covered entities, with the exception of OTRB owner/operators, as part of their CRM Program to conduct cybersecurity evaluations (CSE), have a Cybersecurity Operational Implementation Plan (COIP), a CIRP, and a Cybersecurity Assessment Plan (CAP). The implementation process of these components would be completed by individuals with specialized cybersecurity or information technology experience and expertise (as described in Chapter 2), and would include functions such as (but not limited to) data backups, actions related to critical systems, and architectural design review. There are also additional requirements related to the CIRP that apply to the covered owner/operators that contribute to the costs and benefits of the proposed rule. All covered entities, with the exception of OTRB owner/operators, would also be required to submit names and POC information on

corporate cybersecurity coordinators and alternates. In addition, Pipeline owner/operators would be required to submit names and POC information of physical security coordinators and alternates to TSA. Finally, all covered entities, with the exception of OTRB owner/operators, would submit to TSA, as part of their CRM Program, the CSE, COIP, CIRP, and CAP. Specifically, for the COIP, each covered owner/operator would be required to submit their COIP to TSA for approval no later than 90 calendar days after this rule is published in final form in the Federal Register. Additionally, an owner/operator may request permission from TSA to amend its COIP no later than 45 calendar days before the date it proposes the amendment to become effective, after which TSA will have 30 calendar days to either approve or deny the request to amend the program.

The type of professional skills necessary varies by the proposed requirement. TSA assumes that cybersecurity training programs, incident reports, physical security or cybersecurity coordinator packages, or other similar information submitted to TSA or CISA would be completed by management-level personnel. Any plans associated with an owner/operator's CRM program and submitted to TSA would be completed by individuals with cybersecurity or information technology expertise and undergo a corporate legal review. TSA also assumes that owner/operators would have a manager prepare before a compliance inspection and estimates the cost of this time spent based on a management personnel compensation rate. To calculate costs, TSA uses a relevant average compensation rate for each industry. TSA also assumes the recordkeeping requirements of the rule would be fulfilled by employees with administrative and clerical skills and bases its cost estimate on administrative and clerical personnel compensation rates.

6.7 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 Office of the National Cyber Director (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.

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 CISA's 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 the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA). TSA notes potential differences in terminology and policy as compared to those rulemakings; although the 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.

For pipeline owner/operators, TSA would 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.

TSA also issued SDs in 2021, 2022, mostly recently renewed in 2023 and 2024 in response to

cybersecurity risks to designated freight railroads, passenger rail and rail transit owner/operators, and pipeline owner/operators. In addition, TSA 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 measures.[490] In response to TSA's SDs, many affected owner/operators have taken action, incurred costs, and started to implement many of the cybersecurity risk management program elements that are required in the proposed rule.

TSA recognizes that some of the rule provisions may have already been implemented through current industry cybersecurity practices or in response to TSA's security directives (SDs) and thus a portion of the costs may have already been incurred. However, TSA is assuming a zero baseline which does not account for such actions; but does provide an accounting of costs for requirements captured by SDs and a sensitivity analysis that considers possible existing industry efforts on key cost drivers.

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 National American Electric Reliability Corporation (NERC). TSA has committed to reducing the impact on these multi-sector companies by aligning the agency's proposed requirements with the NIST Cybersecurity Framework, which is also used by the Department of Energy, FERC, and NERC.[491]

---

[490] *See* Information Circular: Surface Transportation IC-2021-01: Enhancing Surface Transportation Cybersecurity at https://www.tsa.gov/sites/default/files/20211201_surface-ic-2021-01.pdf. Accessed on Oct. 19, 2022. Information Circular applicability indicates freight rail, PTPR, and OTRB.

[491] *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).

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 the CIRCIA[492] 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 proposed rule and CIRCIA 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 the proposed rule would be required to make their reports to CISA. TSA is committed to working with CISA to 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. At this time, 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.

[492] Division Y of Pub. L. No. 117-103, 136 Stat. 49 (March 15, 2022).

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

TSA considered 3 other feasible alternatives, detailed in Section 6, in addition to the proposed rule. Alternative 1 would have lower costs than the proposed rule to all covered entities, including small entities, and is discussed below. Alternative 2 would have fewer covered entities than the proposed rule, including small entities, and is discussed below. Alternative 3 would have higher costs and the same number of covered entities as the proposed rule, and is not discussed below.

6.8.1 Alternative 1: Implement a Limited Scope of Requirements

TSA considered a regulatory alternative that would have limited the scope of requirements to including the identification of responsible persons for owner/operators, identification of critical cybersecurity systems, reporting of cybersecurity incidents, and the creation of a CIRP for each owner/operator. More specifically, these requirements identify responsible persons and organizations for an owner/operators' CRM program, identify the owner/operators' 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 at a reactionary level, but it would eliminate visibility of any preventative efforts owner/operators are undertaking.

Unlike the proposed rule, Alternative 1 would have no per employee costs, as well as a reduction in the number of per entity costs. In Table 6-12, TSA presents the cost per entity for freight rail owner/operators under Alternative 1. TSA leverages the respective hour burdens and

compensation rates from Table 6-2 for the requirements retained under this alternative.

Table 6-12: Total Cost per Small Freight Rail Owner/Operator-Alternative 1

Requirement	Unit Time (hours)	Hourly Wage Rate	Unit Cost
	a	b	c = b x a
Familiarization	14.66	$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**

Note: Totals may not add due to rounding.

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. In Table 6-13, TSA presents the cost per entity for pipeline owner/operators.

Table 6-13: Total Cost per Small Pipeline Owner/Operator-Alternative 1

Requirement	Unit Time (hours)	Hourly Wage Rate	Unit Cost
	a	b	c = b x a
Familiarization	56	$126.67	$7,093
Cybersecurity Incident Reporting	3.48	$94.55	$329
CRM Program	87	$119.38	$10,386
CIRP	300	$89.84	$26,953
Cost per Entity			**$44,761**

Note: Totals may not add due to rounding.

Under Alternative 1, 90 percent of affected small entities would be impacted by less than 1 percent of annual revenue, and none of the covered entities have an impact greater than 10 percent in the highest cost year. Table 6-14 presents the costs as a percentage of total annual revenue in the highest cost year under Alternative 1.

Table 6-14: Revenue Impact on Affected Small Entities, Total (Alternative 1)

Revenue Impact Range	Number of Affected Small Entities[1]	Percentage of Affected Small Entities
0% < Impact ≤ 1%	77	97.5%
1% < Impact ≤ 3%	2	2.5%
3% < Impact ≤ 5%	0	
5% < Impact ≤ 10%	0	
Above 10%	0	
Total	**79**	**100%**

Note: Totals may not add due to rounding.

Although this alternative has smaller 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 as a whole. This alternative would not require visibility or accountability of NIST "detect" or "protect" elements whose implementation, as part of a cyber-risk management program, would help prevent malicious actors from exploiting vulnerabilities as well as ensure the confidentiality, availability, 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 requires 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.

6.8.2 Alternative 2: Reduction in Applicability Across the Industries

This alternative would limit the applicability of the requirements to the largest and most critical

owner/operators in each of the regulated industries:

- Freight Railroads: Class I Railroads, as defined by Surface Transportation Board;
- PTPR: Owner/operators that host Class I Freight Rail Lines or those with an average daily ridership of 100,000 passengers over the last five years or in any future year;
- OTRB Owner/operators that meet the criteria for inclusion or applicability of the proposed rule as described in § 1584.107; and
- Pipelines: 100 most critical owner/operators of hazardous liquid and natural gas pipelines and liquefied natural gas facilities.[493]

Under the limited applicability, Alternative 2 would cover six Class I freight rail owner/operators, 27 PTPR agencies, 71 OTRB owner/operators, and 100 pipeline owner/operators in the tenth year of the rule. 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 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. This is depicted in Table 6-15.

[493] Under section 1557(b) of the 9/11 Act, TSA is required to identify the 100 most critical pipeline owner/operators. Due to the sensitive nature of the information used to identify these owner/operators, TSA would individually notify each that they are a designated critical operation subject to the requirements of the proposed alternative.

Table 6-15: Revenue Impact on Affected Small Entities, Total (Alternative 2)

Revenue Impact Range	Number of Affected Small Entities Under Alternative 2	Percentage of Affected Small Entities Under Alternative 2	Number of Affected Small Entities Under Preferred Alternative	Percentage of Affected Small Entities Under Preferred Alternative
0% < Impact ≤ 1%	60	100%	68	86.1%
1% < Impact ≤ 3%			3	3.8%
3% < Impact ≤ 5%			4	5.1
5% < Impact ≤ 10%			2	2.5
Above 10%			2	2.5
Total	**60**	**100%**	**79**	**100%**

Note: Totals may not add due to rounding.

From an RFA perspective, this alternative impacts fewer small entities than the proposed rule. However, TSA did not select this alternative because not requiring cybersecurity mitigation on removed entities can still lead to severe impacts and potentially reduce cybersecurity on the broader sector which play in the supply chain, movement of people and goods, and the economy as a whole. 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 Strategic Rail Corridor Network (STRACNET), are critical to the transportation industry. A cyber-incident on one of these railroads, even a small one, 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 cyber-incident affect their capacity 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, such small entities play a vital role in the larger transportation system and thus should be covered under the rule.

6.9 Sensitivity Analysis of Cost Impacts on Small Entities

TSA recognizes the estimated costs of the proposed rule could potentially have a large impact on smaller entities across transportation modes. However, TSA also recognizes there is some uncertainty surrounding its cost estimates including to what degree entities may already be performing actions that would satisfy the proposed rule. As a result, TSA performed a sensitivity analysis of the major cost drivers (see Section 3.8) to help understand and evaluate the practical impacts of the rule versus the zero-baseline assumption used in the primary analysis. In addition, the primary analysis uses average values across all covered entities, and all cost impact are not distributed uniformly, as larger entities may have larger costs relative to smaller entities. The following section estimates the proposed rule potential impact on small entities using cost values from the sensitivity analysis.

The major cost drivers of the proposed rule include access control costs, cybersecurity system data backups, and cybersecurity training. The remaining costs of the proposed rule stay the same. As discussed in Section 3.8, 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. For the partial compliance group, TSA reduces the cost values for these three costs by 50 percent, while holding all other costs the same. TSA uses these revised estimates to re-evaluate the cost impact of the rule as a percentage of small entity revenue. This was applied to all modes in the sensitivity analysis, although only freight rail and pipelines modes are shown below, as they are the only modes with significant costs (greater than 1% of annual revenue) to small entities.

TSA estimates the costs to small entities under the sensitivity analysis assumptions to be the sum of the cost per employee multiplied by the average number of employees for small entities plus the average cost per entity, by mode. For freight rail entities, TSA estimates the cost per small

entity to be $128,709.[494] For pipeline entities, TSA estimates the cost per small entity to be $185,237.[495] TSA did not conduct an IRFA sensitivity analysis on OTRB entities, as the costs to small OTRB entities does not change under the sensitivity analysis assumptions, nor was one done for PTPR entities, as none of them are small entities.

6.9.1 Cost Impact on Small Freight Rail Entities as Percentage of Revenue

To estimate the impact of the proposed rule, TSA divides the highest estimated cost year of the proposed rule, which in this case is year ten, by reported annual revenue for each of the 17 small freight rail entities (that had full information available). This provides the estimated percentage of revenue impact the proposed rule would have on identified small entities using sensitivity analysis cost values. Table 6-16 presents the number and percentage of small freight rail entities by their level of impact based on annual revenues.

Table 6-16: Number of Affected Small Freight Rail Entities by Revenue Impact (Partial Baseline)

Revenue Impact Range	Number of Affected Small Freight Rail Entities	Percentage of Affected Small Freight Rail Entities
0% < Impact ≤ 1%	13	76.5%
1% < Impact ≤ 3%	2	11.8%
3% < Impact ≤ 5%		
5% < Impact ≤ 10%	2	11.8%
Above 10%		
Total	**17**	**100%**

Note: Totals may not add due to rounding.

As compared to the primary analysis (see Table 6-3), the assumptions under the sensitivity analysis reduces the number of affected small freight rail entities with cost impact greater than 1

[494] The cost per entity (without cost per employee) is estimated to be $100,557.08, the cost per employee is $290.35, and the average number of employees is 96.96 for small freight rail entities. $128,709 = $100,557.08 + ($290.35 × 96.96).

[495] The cost per entity (without cost per employee) is estimated to be $69,975.21, the cost per employee is $589.34, and the average number of employees is 195.6 for small pipeline entities. $185,237.06 = $100,557.08 + ($290.35 × 96.96).

percent of revenue from 11 to four. The number of entities with impact greater than 10 percent of revenue falls from 2 to zero.

6.9.2 Cost Impact on Small Pipeline Entities as Percentage of Revenue

TSA divides the estimated tenth (highest cost) year cost of the proposed rule by reported annual revenue for each of the 7 small pipeline entities. This provides the estimated percentage of revenue impact the proposed rule would have on identified small entities using sensitivity analysis cost values. Table 6-17 presents the number and percentage of small pipeline entities by their level of impact based on annual revenues.

Table 6-17: Number of Affected Small Pipeline Entities by Revenue Impact (Partial Baseline)

Revenue Impact Range	Number of Affected Small Pipeline Entities	Percentage of Affected Small Pipeline Entities
0% < Impact ≤ 1% 1% < Impact ≤ 3% 3% < Impact ≤ 5% 5% < Impact ≤ 10% Above 10%	7	100%
Total	**7**	**100%**

Note: Totals may not add due to rounding.

As compared to the primary analysis (see Table 6-10), the assumptions under the sensitivity analysis have lower costs, but have no impact on the number of affected small pipeline entities. Both the primary analysis and sensitivity analysis estimate costs for small entities to be less than 1% of revenue.

7 PAPERWORK REDUCTION ACT

The Paperwork Reduction Act of 1995 (PRA) (44 U.S.C. 3501. et seq.) requires that Federal agencies consider the impact of paperwork and other information collection burdens imposed on the public and, under the provisions of PRA section 3507(d), obtain approval from the Office of Management and Budget (OMB) for each collection of information it conducts, sponsors, or requires through regulations. 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. Accordingly, TSA has submitted all information requirements to OMB for its review. This section provides the description of the information collection; the respondents impacted by the ICR, and the corresponding time burden it takes TSA to collect said information.

7.1 Description of Information Collection Activities

This proposed rule requires the following activity collections for covered freight rail, PTPR, and pipeline owner/operators:

- Conduct and submit the results of a Cybersecurity Evaluation (CSE)
- Develop and submit a Cybersecurity Operational Integration Program (COIP) to TSA
- For entities that do not have an approved COIP, develop and submit a Plan of Action & Milestones (POAM).
- Identify and submit the accountable executive information
- Identify and submit the cybersecurity coordinator and an alternate information

- Identify Critical Cyber Systems and submit with COIP
- Submit information regarding how the entity is addressing supply chain risk management
- Develop and submit a Cybersecurity Training Plan
- Document Cybersecurity Training (Recordkeeping)
- Report Cybersecurity Incidents to CISA
- Develop a Cybersecurity Implementation Response Plan (CIRP)
- Conduct a test of the CIRP and submit the results to TSA
- Develop and submit a Cybersecurity Assessment Plan (CAP)
- Conduct annual testing of the CAP and submit the results to TSA
- Compliance recordkeeping

Pipelines have the additional collections associated with (1) designating a physical security coordinator and (2) reporting physical security incidents to TSA. OTRB owner/operator have the additional requirement to report cybersecurity incidents to CISA.

7.2 Description of Respondents

Respondents are entities operating as freight rail, PTPR, OTRB, or pipeline owner/operators meeting the following criteria.

Freight rail owner/operators:

- Is a Class I railroad as defined in current 49 CFR 1580.3; or
- Is a Class II or III railroads that:
    - Transports one or more of the categories and quantities of Rail Security-Sensitive Materials in a High Threat Urban Area;
    - 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 years before the effective date of the final rule or in any calendar year after the effective date;
- Is designated as a Defense Connector Railroad by DoD; 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.

PTPR owner/operators:

- Amtrak (also known as the National Railroad Passenger corporation) or 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 railroads that hosts a Class I railroad or Amtrak, regardless of ridership volume; or
- 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.

OTRB owner/operators:

Section § 1584.107 details the criteria for inclusion or applicability of the proposed rule for over-the-road-buses (OTRBs).

Pipeline owner/operators:

- The hazardous liquid pipelines are subject to 49 CFR part 195 and—

- Annually deliver 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
- Are 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;[496]

- Operate a primary control room that is responsible for multiple systems 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; or

- Have a contract with the Defense Logistics Agency to supply hazardous liquids in excess of 70,000 barrels annually.[497]

    - For owner/operators of natural gas and other gas pipelines, the criteria and thresholds were developed by TSA specifically for this proposed rule. The criteria are similar to that used by TSA to identify critical pipeline operators, based on risk, as set forth in the statutory requirement to identify the 100 most critical pipeline operators.[498] The proposed CRM program requirements includes each company that:

- The natural and other gas systems are subject to 49 CFR part 192 and—

[496] *See* proposed 49 CFR part 1586 for a definition of High Consequence Area and a discussion of Terms in subsection D of this section.

[497] The criteria for 70,000 barrels is pending coordination with the Defense Logistics Agency. This amount conforms to what TSA uses to identify critical pipeline systems ("Top 100").

[498] *See* 6 U.S.C. 1207(b).

- 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;
- Delivered natural or other gas to 275,000 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
- For natural gas transmission, have in excess of 200 segment miles that could affect a High Consequence Area;

- Operate a primary control room responsible for multiple systems and the total annual delivery for those systems combined is greater than 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; or
- Provide natural gas service to greater than 275,000 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.
- For owners/operators of Liquefied Natural Gas (LNG) facilities, the proposed CRM program apply to facilities that import LNG or that serve as peak shaving facilities.

7.2.1 Number of Respondents

As discussed in Section 2.1, TSA estimates 293 entities across all modes would initially be covered by the rule in year one and considered respondents. Based on growth rates discussed in

Section 2.2, this value will grow over the next 3 years as shown in Table 2-1. This results in an average number of 296 respondents per year. A distribution of respondents for each industry is depicted in Table 7-1.

Table 7-1: Respondents per Year

Respondents	Year 1	Year 2	Year 3	3-Year Total	Average Annual
Freight Rail	73.0	73.6	74.1	220.7	73.6
PTPR	34.0	34.7	35.5	104.3	34.8
OTRB	71.0	72.8	74.6	218.4	72.8
Pipelines	115.0	115.0	115.0	345.0	115.0
Total Number of Respondents	**293.0**	**296.1**	**299.2**	**888.3**	**296.1**

Note: Totals may not add due to rounding.

7.2.2 Number of Responses

The proposed rule has 18 separate information collection activities covered by the PRA, as shown in Table 7-2. Each of these activities are described in detail in Chapter 3. For many of the provisions, respondents only have to submit one response per year. The number of responses is then calculated by multiplying the rate of one response per entity by the number of entities (with assumed growth post Year 1). For instance, the Cybersecurity Evaluation is submitted every year and then multiplied by the 73 freight rail, 34 PTPR, and 115 Pipeline covered entities. This calculation is then repeated for Years 2 and 3 and the results are summed together and divided by three years to calculate the average annual number of Cybersecurity Evaluation response. This is the same calculation for submitting updated COIP, annual identification of critical cybersecurity systems, supply chain management, reporting physical security incidents to TSA (pipelines only), cybersecurity training documentation and recordkeeping, reporting cybersecurity incidents to CISA, CIRP testing reporting, cybersecurity assessment plan (CAP) submission, CAP annual report of COIP testing, and recordkeeping.

A similar process is followed for the remaining collections. However, the response per respondent (submission rate) may change for each collection. Specifically, all of the covered

entities will submit accountable executive and cybersecurity coordinator information, initial cybersecurity training plan submission, COIP, and CIRP submission in the Year 1, but due to turnover and growth, TSA estimates a small number of those submissions in Years 2 and 3. TSA also estimates 20% of covered entities will submit a POAM.

7.3 Annual Burden Estimate

Over the next three years, TSA estimates the total time burden for conducting the information collection activities would be 352,020 hours, an average of 117,340 hours per year. Table 7-2 displays the annual number of hours for each information collection activity based on the estimated time burdens for each activity described in Chapter 3. For each of the collections, the time burden is calculated by multiplying the time per response by the number of responses per year as show in Table 7-2. The Cybersecurity Evaluation, for instance, is calculated by taking the 40 hours needed for a response (120 for pipeline) (shown in Column a of Table 7-2) and multiplying it by the 73 freight, 34 PTPR, and the 115 Pipeline covered entities (shown in Column b of Table 7-2). This calculation is then repeated for Years 2 and 3 and the results are summed together as shown in Column e of Table 7-2 with the average annual response following in Column f. This same process of multiplying the hour burden times response per covered entity is followed for the remaining collections. The time burden for each collection is then added together for the total burden identified above.

TSA estimates the resulting 3-year total number of responses to be 1,606,115 with an average of 535,372 responses per year. A breakdown of responses per collection for each industry is depicted in Table 7-2.

Table 7-2: PRA Time Burdens

Information Collection Activity by Mode	Number of Responses			Time Per Response (hours)	Time Burden			3-Year Time Burden	Average Annual Time Burden/Responses
	Year 1	Year 2	Year 3		Year 1	Year 2	Year 3		
	A	B	C	D	E = A × D	F = B × D	G = C × D	H = E + F + G	I = H ÷ 3
Cybersecurity Evaluation (CSE)									
Freight Rail	73.00	73.6	74.1	40.00	2,920	2,943	2,966	8,828	2,943
PTPR	34.00	34.7	35.5	40.00	1,360	1,390	1,420	4,170	1,390
Pipelines	115.00	115.00	115.00	120.00	13,800	13,800	13,800	41,400	13,800
Submit COIP									
Freight Rail	73.00	-	0.6	40.00	2,920	-	24	2,944	981
PTPR	34.00	-	0.7	40.00	1,360	-	28	1,388	463
Pipelines	115.00	-	-	40.00	4,600	-	-	4,600	1,533
Update COIP									
Freight Rail	-	73	73.6	13.30	-	971	978	1,949	650
PTPR	-	34	34.7	13.30	-	452	462	914	305
Pipelines	-	115	115	13.30	-	1,530	1,530	3,059	1,020
Initial Identification of Critical Cyber Systems									
Freight Rail	73.00	0.57	0.57	160.00	11,680	91	91	11,862	3,954.13
PTPR	34.00	0.74	0.77	160.00	5,440	118	123	5,682	1,893.87
Pipelines	115.00	-	-	160.00	18,400	-	-	18,400	6,133.33
Annual Identification of Critical Cyber Systems									
Freight Rail	73.00	73.00	73.57	40.00	2,920	2,920	2,943	8,783	2,927.60
PTPR	34.00	34.74	35.51	40.00	1,360	1,390	1,420	4,170	1,390.00
Pipelines	115.00	115.00	115.00	40.00	4,600	4,600	4,600	13,800	4,600.00
Submit POAM									
Freight Rail	14.60	14.71	14.83	80.00	1,168	1,177	1,186	3,531	1,177
PTPR	6.80	6.95	7.10	80.00	544	556	568	1,668	556
Pipelines	23.00	23.00	23.00	80.00	1,840	1,840	1,840	5,520	1,840
Accountable Executive Information Submission									
Freight Rail	73.00	3.51	3.55	3.00	219	11	11	240	80
PTPR	34.00	5.24	5.37	3.00	102	16	16	134	45
Pipelines	115.00	15.72	15.72	3.00	345	47	47	439	146
Cybersecurity Coordinator Information Submission									
Freight Rail	146.00	7.03	7.07	2.00	292	14	14	320	107
PTPR	68.00	10.48	10.74	2.00	136	21	21	178	59
Pipelines	230.00	31.44	31.44	2.00	460	63	63	586	195
Supply Chain Management									
Freight Rail	73.00	73.57	74.14	10.00	730	736	741	2,207	736
PTPR	34.00	34.74	35.51	10.00	340	347	355	1,043	348
Pipelines	115.00	115.00	115.00	10.00	1,150	1,150	1,150	3,450	1,150
Physical Security Coordinator Information Submission									
Pipelines	261.05	35.69	35.69	0.50	131	18	18	166	55
Report Physical Security Incidents to TSA									
Pipelines	2,908.35	2,908.35	2,908.35	0.05	145	145	145	436	145
Initial Cybersecurity Training Plan Development and Submission									
Freight Rail	73.00	0.57	0.57	80.00	5,840	46	46	5,931	1,977
PTPR	34.00	0.74	0.77	80.00	2,720	59	62	2,841	947
Pipelines	115.00	-	-	80.00	9,200	-	-	9,200	3,067
Cybersecurity Training Documentation Recordkeeping									
Freight Rail	134,504.00	135,068.91	135,636.21	0.02	2,690	2,701	2,713	8,104	2,701
PTPR	344,632.00	348,457.42	352,325.29	0.02	6,893	6,969	7,047	20,908	6,969
Pipelines	45,908.00	46,192.63	46,479.02	0.02	918	924	930	2,772	924

Information Collection Activity by Mode	Number of Responses			Time Per Response (hours)	Time Burden			3-Year Time Burden	Average Annual Time Burden/Responses
	Year 1	Year 2	Year 3		Year 1	Year 2	Year 3		
	A	B	C	D	E = A × D	F = B × D	G = C × D	H = E + F + G	I = H ÷ 3
Report Cybersecurity Incidents to CISA									
Freight Rail	10.22	10.31	10.39	1.00	10	10	10	31	10
PTPR	14.96	15.29	15.62	1.00	15	15	16	46	15
OTRB	14.91	15.28	15.66	1.00	15	15	16	46	15
Pipelines	400.20	400.20	400.20	1.00	400	400	400	1,201	400
Cybersecurity Incident Response Plan (CIRP)									
Freight Rail	73.00			80.00	5,840	-	-	5,840	1,947
PTPR	34.00			80.00	2,720	-	-	2,720	907
Pipelines	115.00			80.00	9,200	-	-	9,200	3,067
CIRP Testing									
Freight Rail	73.00	73.57	74.14	120.00	8,760	8,828	8,897	26,485	8,828
PTPR	34.00	34.74	35.51	120.00	4,080	4,169	4,261	12,510	4,170
Pipelines	115.00	115.00	115.00	120.00	13,800	13,800	13,800	41,400	13,800
Cybersecurity Assessment Plan (CAP)									
Freight Rail	73.00	73.57	74.14	44.00	3,212	3,237	3,262	9,711	3,237
PTPR	34.00	34.74	35.51	44.00	1,496	1,529	1,562	4,587	1,529
Pipelines	115.00	115.00	115.00	44.00	5,060	5,060	5,060	15,180	5,060
CAP Annual Report of COIP Testing									
Freight Rail	73.00	73.57	74.14	30.00	2,190	2,207	2,224	6,621	2,207
PTPR	34.00	34.74	35.51	30.00	1,020	1,042	1,065	3,128	1,043
Pipelines	115.00	115.00	115.00	30.00	3,450	3,450	3,450	10,350	3,450
Recordkeeping									
Freight Rail	73.00	73.57	74.14	2.00	146	147	148	441	147
PTPR	34.00	34.74	35.51	2.00	68	69	71	209	70
Pipelines	115.00	115.00	115.00	2.00	230	230	230	690	230
Total Responses	**531,806**	**535,009**	**539,745**					**1,606,115**	**535,372**
Total Time Burden (Hours)					**168,935**	**91,254**	**91,831**	**352,020**	**117,340**

Note: Totals may not add due to rounding.

As required by the PRA (49 U.S.C. 3507(d)), TSA has submitted a copy of the proposed rule to the OMB for its review of the collection of information. In accordance with the 44 U.S.C. 3506(c)(2)(A), TSA solicits public comment on the proposed collection of information to help us determine the usefulness of the information; whether it can help us perform our functions better; whether it is readily available elsewhere; how accurate our estimate of the burden of collection is; the validity of our methods for determining the burden; how TSA can improve the quality, usefulness, and clarity of the information; and how the agency can minimize the burden of collection.

If you submit comments on the collection of information, submit them both to OMB and to the Docket Management Facility where indicated under ADDRESSES, by the date under DATES. Individuals do not need to respond to a collection of information unless it displays a currently valid control number from OMB. Before the requirements for this collection of information becomes effective, TSA will publish a final rule in the *Federal Register* with the valid control number.

8 INTERNATIONAL TRADE IMPACT ASSESSMENT

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

9 UNFUNDED MANDATES REFORM ACT ANALYSIS

Title II of UMRA, Pub. L. 104–4, 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 of the UMRA, TSA generally must 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 ($177 million adjusted for inflation) or more in any year.[499] Before TSA promulgates a rule for which a written statement is required, Section 205 of UMRA generally requires TSA to identify and consider a reasonable number of regulatory alternatives and adopt 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 TSA to adopt an alternative other than the least costly, most cost-effective, or least burdensome alternative if the Administrator publishes an explanation with the final rule about why that alternative was not adopted.

Before TSA establishes any regulatory requirements that may significantly or uniquely affect small governments, including Tribal governments, it must develop under Section 203 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 TSA regulatory proposals with significant Federal intergovernmental mandates; and informing, educating, and advising small governments on compliance with the

[499] $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 on September 30, 2023.

regulatory requirements.

Under 2 U.S.C. 1503(5), 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.[500]

[500] *See* National Cybersecurity Strategy (March 2023) at 4 ("The cyber operations of criminal syndicates now represent a threat to the national security, public safety, and economic prosperity of the United States and its allies and partners. Ransomware incidents have disrupted critical services and businesses across the country and around the world, from energy pipelines and food companies, to schools and hospitals. Total economic losses from ransomware incidents continue to climb, reaching billions of U.S. dollars annually. Criminal syndicates often operate out of states that do not cooperate with U.S. law enforcement and frequently encourage, harbor, or tolerate such activities. These and other malicious cyber activities continue to threaten Americans across society, including disproportionately affecting those without the resources necessary to protect themselves, recover, or seek recourse."). This document is available at: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf (last accessed July 20, 2023).

APPENDIX A

Appendix A lists out the major provisions of this proposed CRM rule and how they relate to the current SDs.[501] As discussed throughout the NPRM and this RIA, the majority of provisions exist to some extent within the SDs; distinctions are shown below in the Notes column.

Cyber Risk Management (CRM) Notice of Proposed Rulemaking (NPRM) vs. Cyber Security Directives Requirements							
Provisions Included In CRM NPRM		SECURITY DIRECTIVES					NOTES
		PL-2021-01	PL-2021-02	1580-21-01	1582-21-01	1580/82-21-02	
Cybersecurity Evaluation (CSE)		X		X	X		This provision in the NPRM is more expansive than the assessment required in the SDs.
Cybersecurity Operational Implementation Plan (COIP)			X			X	The SDs required a "CIP," this plan will now be the "COIP" to reflect the additional proposed requirements for the plan.
	Governance of CRM Program						New requirement (Identification of Accountable Executive and Individuals/vendors with Cybersecurity Responsibilities).
	Designation of Cybersecurity Coordinator	X		X	X		
	Identification of Critical Cyber Systems and Network Architecture		X			X	
	Supply Chain Risk Management						New requirement (O/O must incorporate policies, procedures and capabilities to address supply chain cyber vulnerabilities into the COIP).
	Protection of Critical Cyber Systems		X			X	Includes Network Segmentation, Access Control, and patches and software updates.
	Cybersecurity Training						New requirement
	Detection of Cybersecurity Incidents		X			X	Includes detection and monitoring of critical cyber systems.

[501] For reference, heading PL-2021-01 corresponds to Pipeline SD 1, originally issued in May 2021. Heading PL-2021-02 corresponds to Pipeline SD 2, originally issued in July 2021. Heading 1580-21-01 corresponds to Freight Rail SD 1, originally issued in December 2021. Heading 1582-21-01 corresponds to Passenger Rail/Public Transportation SD 1, originally issued in December 2021. And heading 1580/82-21-02 corresponds to Freight Rail SD 2, originally issues in October 2022.

Cyber Risk Management (CRM) Notice of Proposed Rulemaking (NPRM) vs. Cyber Security Directives Requirements						
Provisions Included In CRM NPRM	SECURITY DIRECTIVES					NOTES
	PL-2021-01	PL-2021-02	1580-21-01	1582-21-01	1580/82-21-02	
Capabilities to Respond to A Cybersecurity Incident		X			X	Includes auditing of unauthorized access to internet domains and communication between OT systems and external systems.
Cybersecurity Incident Reporting	X		X	X		
Cybersecurity Incident Response Plan (CIRP)		X	X	X		
Plan of Action and Milestones (POAM)	X		X	X		Incorporating a POAM in the COIP aligns with the identification of remediation measures under Vulnerability Assessments in the SD01 series.
Cybersecurity Assessment Plan (CAP)		X			X	
Annual Report of Assessment Findings		X			X	