BILLING CODE 9110-05-P

DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

[Docket No. TSA-2022-0001]

RIN 1652-AA74

49 CFR Chapter XII

Enhancing Surface Cyber Risk Management

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

ACTION: Advance notice of proposed rulemaking.

SUMMARY: The Transportation Security Administration (TSA) is seeking input regarding ways to strengthen cybersecurity and resiliency in the pipeline and rail (including freight, passenger, and transit rail) sectors. This advance notice of proposed rulemaking (ANPRM) offers an opportunity for interested individuals and organizations, particularly owner/operators of higher-risk pipeline and rail operations, to help TSA develop a comprehensive and forward-looking approach to cybersecurity requirements. TSA is also interested in input from the industry associations representing these owners/operators, third-party cybersecurity subject matter experts, and insurers and underwriters for cybersecurity risks for these transportation sectors. Although TSA will review and consider all comments submitted, we are specifically interested in responses to the questions posed in this ANPRM. Input received in response to this ANPRM will assist TSA in better understanding how the pipeline and rail sectors implement cyber risk management (CRM) in their operations and will support us in achieving objectives related to the enhancement of pipeline and rail cybersecurity.

DATES: Submit comments by **[INSERT DATE 45 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

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

- *Electronic Federal eRulemaking Portal*: https://www.regulations.gov. Follow the online instructions for submitting comments.
- *Mail*: Docket Management Facility (M-30), U.S. Department of Transportation, 1200 New Jersey Avenue SE, West Building Ground Floor, Room W12-140, Washington, DC 20590-0001. The Department of Transportation (DOT), which maintains and processes TSA's official regulatory dockets, will scan the submission and post it to FDMS. Comments must be postmarked by the date indicated above.
- *Fax*: (202) 493-2251.

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

FOR FURTHER INFORMATION CONTACT: *For program questions*: Victor Parker, Surface Division, Policy, Plans, and Engagement, TSA-28, Transportation Security Administration, 6595 Springfield Center Drive, Springfield, VA 20598-6002; telephone (571) 227-1039; email: VettingPolicy@tsa.dhs.gov. *For legal questions*: David Kasminoff (TSA, Senior Counsel, Regulations and Security Standards) at telephone (571) 227-3583, or e-mail to VettingPolicy@tsa.dhs.gov.

SUPPLEMENTARY INFORMATION:

Comments Invited

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

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

If you would like TSA to acknowledge receipt of comments submitted by mail, include with your comments a self-addressed, stamped postcard on which the docket number appears. TSA will stamp the date on the postcard and mail it to you.

All comments, except those that include confidential or sensitive security information (SSI)[1] will be posted to https://www.regulations.gov, and will include any personal information you have provided. Should you wish your personally identifiable information redacted prior to filing in the docket, please clearly indicate this request in your submission to TSA. TSA will consider all comments that are in the docket on or

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

before the closing date for comments and will consider comments filed late to the extent practicable. The docket is available for public inspection before and after the comment closing date.

Handling of Certain Sensitive Information Submitted in Public Comments

Do not submit comments that include trade secrets, confidential commercial or financial information, SSI, or protected critical infrastructure information to the public regulatory docket. Comments containing this type of information should be submitted separately from other comments, appropriately marked as containing such information, and submitted by mail to the address listed in **FOR FURTHER INFORMATION CONTACT** section. TSA will take the following actions for all submissions containing SSI:

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

Reviewing Comments in the Docket

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

You may review TSA's electronic public docket at http://www.regulations.gov. In addition, DOT's Docket Management Facility provides a physical facility, staff, equipment, and assistance to the public. To obtain assistance or to review comments in TSA's public docket, you may visit this facility between 9 a.m. and 5 p.m., Monday through Friday, excluding legal holidays, or call (202) 366-9826. This DOT facility is located in the West Building Ground Floor, Room W12-140 at 1200 New Jersey Avenue SE, Washington, DC 20590.

Availability of Rulemaking Document

You can find an electronic copy of rulemaking documents relevant to this action by searching the electronic FDMS web page at https://www.regulations.gov or at https://www.federalregister.gov.

In addition, copies are available by writing or calling the individual in the **FOR FURTHER INFORMATION CONTACT** section. Make sure to identify the docket number of this ANPRM.

Abbreviations and Terms Used in This Document

ANPRM – Advance notice of proposed rulemaking

AAR – Association of American Railroads

APTA – Association of Public Transportation Agencies

ATSA – Aviation and Transportation Security Act

C2M2 – Cybersecurity Capabilities Maturity Model

CFATS – Chemical Facility Anti-Terrorism Standards

CFSR – Critical facility security reviews

CIP – Critical Infrastructure Protection

CISA – Cybersecurity and Infrastructure Security Agency

CRM – Cyber risk management

CSR – Corporate Security Reviews

DFARS – Defense Federal Acquisition Regulation Supplement

FERC – Federal Energy Regulatory Commission

FRA – Federal Railroad Administration

FSB – Russian Federal Security Service

DHS – Department of Homeland Security

DOE – Department of Energy

DOT – Department of Transportation

ICS – Industrial Control System

IT – Information technology

NERC – North American Electric Reliability Corporation

NIST – National Institute of Standards and Technology

NPRM – Notice of proposed rulemaking

OT – Operational technology

RBPS – Risk-Based Performance Standard

SCADA – Supervisory control and data acquisition

SSI – Sensitive security information

TSA – Transportation Security Administration

I. Introduction

A. Pipeline transportation

The national pipeline system consists of more than 3.3 million miles of networked pipelines transporting hazardous liquids, natural gas, and other liquids and gases for energy needs and manufacturing. 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. In addition to portions of the network that are manually operated, the pipeline system includes use of automated industrial control systems (ICS), such as supervisory control and data acquisition (SCADA) systems to monitor and manage the system. 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. Protecting vital supply chain infrastructure of pipeline operations is critical to national security and commerce.

B. Rail transportation

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

1. Freight Railroads

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 seven Class I railroads and 580 local (also known as Short Line) railroads and 21 regional railroads. The Class I railroads had 2021 operating revenues of at least $900 million. These seven 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.[2] As stated by the American Association of Railroads (AAR), the freight rail sector provides "a safe, efficient, and cost-effective transportation network that reliably serves customers and the nation's economy."[3]

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, railroads are subject to safety regulations promulgated and enforced by the Federal Railroad Administration (FRA). TSA administers and enforces rail security regulations contained in 49 CFR part 1580.

2. Passenger railroads

[2] *See* https://www.aar.org/wp-content/uploads/2020/08/AAR-Railroad-101-Freight-Railroads-Fact-Sheet.pdf (last visited Sep. 19, 2022).
[3] *Id.*

Passenger rail is divided into two categories: inter-city and commuter rail service. Inter-city provides long-distance service, while commuter railroads provide service over shorter distances, usually less than 100 miles. The 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.[4] 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.[5] Nearly half of all Amtrak trains operate at top speeds of 100 mph or greater. In fiscal year 2021, Amtrak customers took nearly 12.2 million trips.[6]

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.[7]

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

---

[4] *See* https://www.apta.com/wp-content/uploads/APTA_Fact-Book-2019_FINAL.pdf (last visited Sep. 19, 2022).
[5] *Id.*
[6] *See* https://www.amtrak.com/content/dam/projects/dotcom/english/public/documents/corporate/nationalfactsheets/Amtrak-Company-Profile-FY2021-030922.pdf at 1 (last visited Sep. 19, 2022).
[7] *Id.* at 3.

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

Amtrak and other passenger railroads also host freight rail operations. In fact, the Northeast Corridor is the busiest railroad in North America, with approximately 2,200 Amtrak, commuter, and freight trains operating over some portion of the Washington-Boston route each day.[8] As with freight railroads, passenger railroads are subject to safety regulations put forth and enforced by the FRA. TSA administers and enforces passenger rail security regulations contained in 49 CFR part 1582.

3. Rail transit

Public transportation in America is critically important to our way of life, as evidenced by the number of riders on the Nation's public transportation systems. According to the American Public Transportation Association (APTA), 2019 Public Transportation Fact Book, there were over 9.97 million unlinked passenger trips in 2019.[9] Nationwide, 7.8 million Americans commute to work on transit, equivalent to approximately five percent of workers. In major metropolitan areas, like New York City, over 31 percent of commuters rely on public transportation for their daily commute.[10] Rail transit is a critical part of this system, representing about 48 percent of trips.[11] A successful cyber-attack would have a profound impact on ridership and a negative economic impact nationwide.

---

[8] *Id.* at 4.
[9] *Id.* at 10.
[10] *See* APTA, 2021 Public Transportation Fact Book at 12, available at https://www.apta.com/wp-content/uploads/APTA-2021-Fact-Book.pdf (last visited Sep. 19, 2022).
[11] 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. *See id.* at 8.

C. Cybersecurity threats

Cyber actors have demonstrated their willingness to engage in cyber intrusions and conduct cyber-attacks[12] against critical infrastructure by exploiting the vulnerability of Operational Technology (OT)[13] and Information Technology (IT)[14] systems. Pipeline and rail systems, and associated facilities, are vulnerable to cyber-attacks due to legacy ICS that lack updated security controls and the dispersed nature of pipeline and rail networks spanning urban and outlying areas.

As pipeline and rail owner/operators[15] begin integrating IT and OT systems into their ICS environment to further improve safety, enable efficiencies, and/or increase automation, the ICS environment increasingly becomes more vulnerable to new and evolving cyber threats. A successful cyber-intrusion could affect the safe operation and reliability of OT systems, including SCADA systems, process control systems, distributed control systems, safety control systems, measurement systems, and telemetry systems.

---

[12] For purposes of this ANPRM, 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* (last visited on Sept. 19, 2022).

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

[14] For purposes of this ANPRM, 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."

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

From a design perspective, some pipeline and rail assets are more attractive to cyber-attack simply because of the transported commodity and the impact an attack would have on national security and commerce. Minor pipeline and rail system disruptions may result in commodity price increases, while prolonged pipeline and rail disruptions could lead to widespread energy shortages and disruption of critical supply lines. Short-and long-term disruptions and delays may affect other domestic critical infrastructure and industries that depend on pipeline and rail system commodities, such as our national defense system.

On May 8, 2021, a major pipeline operator announced that it had halted its pipeline operations due to a ransomware attack,[16] temporarily disrupting supplies of gasoline and other refined petroleum products throughout the East Coast of the United States. This ransomware attack highlighted the potentially devastating impact that increasingly sophisticated cybersecurity events can have on our nation's critical infrastructure, as well as the direct repercussions felt by U.S. citizens.

This May 2021 event is just one of many recent ransomware attacks that have demonstrated the necessity of ensuring that critical infrastructure owner/operators are proactively deploying CRM measures. The need to take urgent action to mitigate the threats facing domestic critical infrastructure, which have important implications for national and economic security, including enhancing the pipeline and rail industry's current cybersecurity risk management posture, is further highlighted by recent warnings about Russian, Chinese, and Iranian state-sponsored cyber espionage campaigns to

[16] Ransomware is a malicious type of cyber-attack where attackers encrypt an organization's data and demand payment to restore access. *See* NIST Guidance on Ransomware at its Small Business Cybersecurity Corner, accessible at https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/ransomware (last visited Sept. 19, 2022).

develop capabilities to disrupt U.S. critical infrastructure to include the transportation sector.[17]

On March 24, 2022, the U.S. Department of Justice unsealed indictments of three Russian Federal Security Service (FSB) officers and employees of a State Research Center of the Russian Federation (FGUP) Central Scientific Research Institute of Chemistry and Mechanics (also known as "TsNIIKhM") for their involvement in intrusion campaigns against U.S. and international oil refineries, nuclear facilities, and energy companies. Documents revealed that the FSB conducted a multi-stage campaign in which they gained remote access to U.S. and international Energy Sector networks, deployed ICS-focused malware, and collected and exfiltrated enterprise and ICS-related data.[18] A recent multi-national cybersecurity advisory noted that "Russian state-sponsored cyber actors have demonstrated capabilities to compromise IT networks; develop mechanisms to maintain long-term, persistent access to IT networks; exfiltrate sensitive data from IT and [OT] networks; and disrupt critical [ICS/OT] functions by deploying destructive malware."[19]

The Nation's adversaries and strategic competitors will continue to use cyber espionage and cyber-attacks to seek political, economic, and military advantage over the

---

[17] *See, e.g.,* the following recent Joint Cybersecurity Advisories available at https://www.cisa.gov/uscert/ncas/alerts: *Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities,* Alert AA21-321A (Nov. 17, 2021); *Sophisticated Spearphishing Campaign Targets Government Organizations, IGOs, and NGOs*, Alert AA21-148A (May 28, 2021); *Tactics, Techniques, and Procedures of Indicted APT40 Actors Associated with China's MSS Hainan State Security Department,* Alert AA21-200A (July 19, 2021); and *Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure,* Alert AA22-011A (Jan. 11, 2022).

[18] *See* Joint Cybersecurity Advisory, *Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector*, Alert AA22-083A (Mar. 25, 2022), available at: https://www.cisa.gov/uscert/ncas/alerts/aa22-083a (last visited Sep. 19, 2022).

[19] *See* Joint Cybersecurity Advisory, *Russian State Sponsored and Criminal Cyber Threat to Critical Infrastructure*, Alert AA22-110A (Apr. 20, 2022), available at: https://www.cisa.gov/uscert/ncas/alerts/aa22-110a (last visited Sep. 19, 2022).

United States and its allies and partners. These recent incidents demonstrate the potentially devastating impact that increasingly sophisticated cybersecurity events can have on our nation's critical infrastructure, as well as the direct repercussions felt by U.S. citizens. The consequences and threats discussed above demonstrate the necessity of ensuring that critical infrastructure owner/operators are proactively deploying CRM measures.

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

Some sectors have taken significant steps to protect either their IT or OT systems, depending on which is considered most critical for their business needs (*e.g.,* a commodities sector may focus on OT systems while a financial sector or other business that focuses on data may focus on IT systems). Ransomware attacks targeting critical infrastructure threaten *both* IT and OT systems and exploit the connections between these systems. For example, when OT components are connected to IT networks, this connection provides a path for cyber actors to pivot from IT to OT systems.[20] Given the importance of critical infrastructure to national and economic security and America's way of life, accessible OT systems and their connected assets and control structures are an attractive target for malicious cyber actors seeking to disrupt critical infrastructure for profit or to further other objectives. As the Cybersecurity and Infrastructure Security Agency (CISA) recently noted, recent cybersecurity incidents demonstrate that intrusions affecting IT systems can also affect critical operational processes even if the intrusion does not directly impact an OT system.[21] For example, business operations on the IT

[20] *See* CISA Fact Sheet, *Rising Ransomware Threat to Operational Technology Assets* (June 2021), available at https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Rising_Ransomware_Threat_to_OT_Assets_508C.pdf (last visited Sep. 19, 2022).
[21] *Id.*

system sometimes are used to orchestrate OT system operations. As a result, when there is a compromise of the IT system, there is a risk of unaffected OT systems being impacted by the loss of operational directives and accounting functions.

DHS, the Department of Energy (DOE), the Federal Bureau of Investigation, and the National Security Agency have all urged the private sector to implement a layered, "defense-in-depth" cybersecurity posture. For example, ensuring that OT and IT systems are separate and segregated will help protect against intrusions that can exploit vulnerabilities from one system to infect another. A stand-alone, unconnected ("air-gapped") OT system is safer from outside threats than an OT system connected to one or more enterprise IT systems with external connectivity (no matter how secure the outside connections are thought to be).[22] By implementing a layered approach, owner/operators and their network administrators will enhance the defensive cybersecurity posture of their OT and IT systems, reducing the risk of compromise or severe operational degradation if their system is compromised by malicious cyber actors.[23]

E. TSA surface-related security directives and information circulars

TSA issued security directives in 2021 and 2022[24] in response to the cybersecurity threat to surface transportation systems and associated infrastructure to protect against the

---

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

[23] *See* Joint Cybersecurity Advisory, Alert AA21-200A, *supra* n. 17.

[24] *See* https://www.tsa.gov/for-industry/surface-transportation-cybersecurity-toolkit for links to the security directives. 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

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."[25] The first pipeline security directive (SD) (the SD Pipeline-2021-01 series) requires several actions to enhance the security of critical pipeline systems[26] against cyber-attacks and provided that owners/operators must: (1) designate a primary and alternate Cybersecurity Coordinator; (2) report cybersecurity incidents to CISA within 24 hours of identification of a cybersecurity incident;[27] and (3) review TSA's pipeline guidelines,[28] assess their current cybersecurity posture, and identify remediation measures to address the vulnerabilities and cybersecurity gaps.[29] For purposes of this requirement, a "cybersecurity incident" is defined as "an event that, without lawful authority, jeopardizes, disrupts or otherwise impacts, or is reasonably likely to jeopardize, disrupt or otherwise impact, the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information residents on the system." The reports must (1) identify the affected systems or facilities; and (2) describe the threat, incident, and impact or potential impact on IT and OT systems and operations.

---

additional duties and powers to the Administrator; and section 114(m) provides authority for the Administrator to take actions that support other agencies.

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

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

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

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

[29] 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.

The second pipeline security directive (the SD Pipeline 2021-02 series), issued on July 26, 2021, required owner/operators to implement specific mitigation measures to protect against ransomware attacks and other known threats to IT and OT systems and conduct a cybersecurity architecture design review. This security directive also required owner/operators to develop and adopt a cybersecurity incident response plan to reduce the risk of operational disruption should their IT and/or OT systems be affected by a cybersecurity incident.[30]

In December 2021, TSA issued security directives to higher-risk freight railroads (the SD 1580-21-01 series)[31] and passenger rail and rail transit owner/operators (the SD 1582-21-01 series),[32] requiring that they also implement the following requirements previously imposed on pipeline systems and facilities: (1) designation of a cybersecurity coordinator; (2) reporting of cybersecurity incidents to CISA within 24 hours; (3) developing and implementing a cybersecurity incident response plan to reduce the risk of an operational disruption; and (4) completing a cybersecurity vulnerability assessment to identify potential gaps or vulnerabilities in their systems. For owner/operators not specifically covered under the SD 1580-21-01 or 1582-2021-02 series, TSA also issued an "information circular" (IC-2021-01), which included a non-binding recommendation for those surface owner/operators not subject to the security directives to voluntarily implement the same measures.[33]

---

[30] *See* https://www.tsa.gov/sites/default/files/sd_pipeline-2021-01b_05-29-2022.pdf (last visited Oct. 19, 2022) for a version of the SD with the prescriptive requirements initially imposed.
[31] *See* https://www.tsa.gov/sites/default/files/sd-1580-21-01a.pdf (last visited Oct. 19, 2022) for the most current version of this SD series.
[32] *See* https://www.tsa.gov/sites/default/files/sd-1582-21-01a.pdf (last visited Oct. 19, 2022) for the most current version of this SD series.
[33] *See* https://www.tsa.gov/sites/default/files/20211201_surface-ic-2021-01.pdf (last visited Oct. 19, 2022).

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 security directive series, effective July 27, 2022 (SD Pipeline 2021-02C), to maintain the security objectives in the previous versions of the security directive but also provide more flexibility by imposing performance-based, rather than prescriptive, security measures. The revised directive allows covered owner/operators to choose how best to implement security measures for their specific systems and operations while mandating that they achieve critical security outcomes. This approach also affords these owner/operators with the ability to adopt new technologies and security capabilities as they become available, provided that TSA's mandated security outcomes are met.

The revised directive specifically requires the covered owner/operators of critical pipeline systems and facilities to take the following actions:

- 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 Cybersecurity Incident Response Plan to reduce the risk of operational disruption, or the risk of other significant impacts on necessary capacity, as defined in the security directive, 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 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.

The Cybersecurity Implementation Plans must identify how the owner/operators will meet the following primary security outcomes:

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

As noted above, in addition to developing and implementing a TSA-approved Cybersecurity Implementation Plan, this directive requires the covered owner/operators to continually assess their cybersecurity posture. These owner/operators must develop and update a Cybersecurity Assessment Program and submit an annual plan to TSA that describes their program for the coming year, including details on the processes and

techniques that they would be using to assess the effectiveness of cybersecurity measures. Techniques such as penetration testing of IT systems and the use of "red" and "purple" team (adversarial perspective) testing are referenced in the SD. At a minimum, the plan must include an architectural design review every two years.

The scope of the requirements in this directive apply to Critical Cyber Systems. TSA defined a Critical Cyber System to include "any IT or OT system or data that, if compromised or exploited, could result in operational disruption. Critical Cyber Systems include business services that, if compromised or exploited, could result in operational disruption." [34]

On October 18, 2022, TSA issued a security directive imposing similar performance-based cybersecurity requirements on higher-risk freight railroads, passenger rail, and rail transit owner/operators (SD 1580/82-2022-01).[35] This security directive was also developed with extensive input from industry stakeholders and federal partners, including CISA and the FRA, to address issues unique to the rail industry.

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

Before issuance of the requirements discussed above, TSA primarily assessed the security posture of pipeline owner/operators by encouraging their voluntary implementation of security recommendations in TSA's Pipeline Security Guidelines. These guidelines were first developed in 2010 and 2011 in collaboration with industry

[34] For purposes of this directive, "operational disruption" means a deviation from or interruption of necessary capacity that results from a compromise or loss of data, system availability, system reliability, or control of a TSA-designated critical pipeline and rail system or facility." Necessary capacity is determined by the owner/operator based on a "determination of capacity to support its business-critical functions required for pipeline and rail operations and market expectations."

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

and government members of the Pipeline Sector and Government Coordinating Councils and industry association representatives and included a range of recommended security measures covering all aspects of pipeline operations. The guidelines are used as the standard for TSA's Pipeline Security Program Corporate Security Reviews (CSRs) and Critical Facility Security Reviews (CFSRs) of the most critical pipeline systems. The CSR program has been in effect since 2003, during which time a total of approximately 260 CSRs have been completed industry-wide. Approximately 800 CFSRs have been completed since this program's inception in 2009.

In 2018, TSA published updated Pipeline Security Guidelines.[36] As part of this update, TSA added Section 7, "Pipeline Cyber Asset Security Measures", including pipeline cyber asset identification; security measures for pipeline cyber assets; and cybersecurity planning and implementation guidance.

While the 2018 guidelines are neither mandatory nor enforceable, the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Act) required the Secretary of Homeland Security (Secretary) to issue and update security recommendations for pipeline security; assess voluntary compliance; and, determine, after consultation with the Secretary of Transportation, whether regulations are appropriate based on the "extent of risk and appropriate mitigation measures."[37] TSA also has general authorities, including its authority to issue regulations and security directives in order to protect transportation security.[38]

---

[36] *See* Pipeline Security Guidelines (March 2018), with Change 1 (April 2021), available at: https://www.tsa.gov/sites/default/files/pipeline_security_guidelines.pdf (last visited Sep. 19, 2022).
[37] *See* section 1557 of Pub. L. 110-53 (121 Stat. 266; Aug. 3, 2007), as codified at 6 U.S.C. 1207.
[38] *See* 49 U.S.C. 114(*l*).

Consistent with theses authorities, TSA has issued cybersecurity SDs applicable to critical pipeline owner/operators, but has not issued regulations under the 9/11 Act's pipeline security provision or under TSA's general authorities, and has not imposed cybersecurity requirements on the full scope of pipeline owner/operators to which the guidelines apply. Although this rulemaking effort is focused specifically on cybersecurity measures, TSA intends to continue to conduct voluntary security assessments in areas where mandatory requirements do not exist (*e.g.*, the physical security measures recommended in the guidelines) as part of a "structured oversight" approach. As part of this approach, TSA assesses industry's voluntary adoption and adherence to non-regulatory guidelines, including Security Action Items and other security measures developed jointly with, and agreed to by, industry stakeholders to meet relevant security needs.

In 2008, TSA promulgated regulations imposing security requirements on owner/operators of rail transit systems, including passenger rail and commuter rail, heavy rail transit, light rail transit, automated guideway, cable car, inclined plane, funicular, and monorail systems. The rule, in pertinent part, covers appointment of security coordinators and security-related reporting requirements. For freight railroads, the 2008 rule also imposed requirements for the secure transport of Rail Security-Sensitive Materials.[39]

In addition to measures to enhance pipeline security, the 9/11 Act required TSA to issue regulations to enhance surface transportation security through security training of frontline employees. The 9/11 Act mandate includes prescriptive requirements for who

[39] *See* Rail Transportation Security Final Rule (Rail Security Rule), 73 FR 72130 (Nov. 26, 2008).

must be trained, what the training must encompass, and how to submit and obtain approval for a training program.[40] The 9/11 Act also mandates regulations requiring higher-risk railroads and over-the-road buses (OTRBs) to appoint security coordinators.[41]

On March 23, 2020, TSA published the final rule, "Security Training for Surface Transportation Employees."[42] This regulation requires owner/operators of higher-risk freight railroad carriers (as defined in 49 CFR 1580.101), public transportation agencies (including rail mass transit and bus systems and passenger railroad carriers (as defined in 49 CFR 1582.101), and OTRB companies (as defined in 49 CFR 1584.101)), to provide TSA-approved security training to employees performing security-sensitive functions. In addition to implementing these provisions, the final rule also defined Transportation Security-Sensitive Materials.[43]

The 9/11 Act also required TSA to issue regulations requiring certain public transportation agencies and rail carriers to conduct security assessments, vulnerability assessments, and security plans.[44] Such assessments and plans must entail, for instance, identification and evaluation of critical information systems[45] and redundant and backup systems needed to ensure continued operations in the event of an attack or other incident and identification of the vulnerabilities to these systems.[46] The vulnerability assessment applicable to high-risk rail carriers must also identify strengths and weaknesses in (1)

---

[40] *See* secs. 1408, 1517, and 1534 of the 9/11 Act, as codified at 6 U.S.C. 1137, 1167, and 1184, respectively.
[41] *See* secs. 1512 and 1531 of the 9/11 Act, codified at 6 U.S.C. 1162 and 1181, respectively.
[42] 85 FR 16456.
[43] *See* sec. 1501(13) of the 9/11 Act, as codified at 6 U.S.C. 1151(13).
[44] *See* secs. 1405 and 1512, as codified at 6 U.S.C. 1134 and 1162, respectively. *See also* section 1521, as codified at 6 U.S.C. 1181 (which imposes similar requirements for OTRBs).
[45] *See* secs. 1405(a)(3) and 1512(d)(1)(A), as codified at 6 U.S.C. 1134(a)(3), 1162(d)(1)(A), respectively.
[46] *See* secs. 1405(c)(2), 1512(d)(1)(D), and 1512(e)(1)(G), as codified at 6 U.S.C. 1134(c)(2), 1162(d)(1)(D), 1162(e)(1)(G), respectively.

programmable electronic devices, computers, or others automated systems used in providing transportation; (2) alarms, cameras, and other protection systems; (3) communications systems and utilities needed for railroad security purposes, including dispatching and notification systems; and (4) other matters determined appropriate by the Secretary.[47] For security plans, the statute requires regulations that address, among other things, the protection of passenger communication systems, emergency response, ensuring redundant and backup systems are in place to ensure continued operation of critical elements of the system in the event of a terrorist attack or other incident, and other actions or procedures as the Secretary determines are appropriate to address the security of the public transportation system or the security of railroad carriers, as appropriate.[48]

In short, the 9/11 Act provisions described above contain a combination of detailed requirements and grants of authority to the Secretary (and ultimately TSA) regarding the content of security training programs, vulnerability assessments, and security plans. Each of these provisions confirms and supplements TSA's authority to impose such requirements as are appropriate or necessary to ensure the security of the applicable systems.

G. Cyber risk management

CRM involves all activities designed to identify and mitigate risk-exposures to cyber technology, both informational and operational, to ensure safe, sustained operations of vital systems and associated infrastructure. DHS defines risk as the "potential for an adverse outcome assessed as a function of threats, vulnerabilities, and consequences

[47] *See* sec. 1512(d), as codified at 6 U.S.C. 1162(d).
[48] *See* secs. 1405(c)(2) and 1512(e), as codified at 6 U.S.C. 1134(c)(2), 1162(e), respectively.

associated with an incident, event, or occurrence."[49] TSA's consideration of cybersecurity risks includes consideration of threat information similar to the information discussed above, emerging intelligence, the need to mitigate the consequences of a cyber-attack, and the inherent vulnerabilities of transportation systems and operations to cybersecurity incidents.

The cybersecurity risks to the transportation sector encompass both the vulnerabilities related to secure and safe operation of vital systems and the consequences of a direct attack or ancillary failure or shutdown of a system due to an inability to isolate and control the impact of a cyber-attack. Existing CRM standards—which are identified in the next section of this ANPRM—address identification, assessment, and mitigation of risk from a variety of sources. Strong CRM generally enhances both security and safety and facilitates operations, protects the sector's entities, and ensures the resiliency of these critical sectors.

H. Existing standards and requirements

Table 1 identifies industry and government standards and guidelines that could be used to develop a CRM program. This list is not exhaustive; incorporating CRM using other existing guidelines or standards may also be appropriate.

Table 1. Cybersecurity standards and sources

Standard	Source[1]
Standards developed by government and government-affiliated agencies	
North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection (CIP) cybersecurity reliability standards, approved by the Federal Energy Regulatory Commission (FERC)	https://www.nerc.com/pa/Stand/Pages/USRelStand.aspx
CISA's Chemical Facility Anti-Terrorism Standards (CFATS)[2]	https://www.cisa.gov/chemical-facility-anti-terrorism-standards

[49] DHS Risk Lexicon, 2010 Edition, at 27, available at: https://www.cisa.gov/sites/default/files/publications/dhs-risk-lexicon-2010_0.pdf (last visited Sep. 19, 2022).

CISA's Cross-Sector Cybersecurity Performance Goals (Common Bassline Controls and sector-specific controls and goals)	https://www.cisa.gov/cpgs
DOE's Cybersecurity Capabilities Maturity Model (C2M2)	https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2
NIST Framework for Improving Critical Infrastructure Cybersecurity	https://www.nist.gov/cyberframework/framework
NIST Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations	https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
Federal Risk and Authorization Management Program (FedRAMP), for Cloud Service Offerings	https://www.fedramp.gov/
International Organization for Standardization /International Electrotechnical Commission 27000 family of standards	https://www.iso.org/standard/73906.html
Standards developed by associations, and private sector organizations	
American Petroleum Institute	https://www.api.org/news-policy-and-issues/cybersecurity
MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®)	https://attack.mitre.org/.
Standards developed for other sectors of the economy, both domestically and internationally, that could be models for requirements in the pipeline and rail sectors	
New York State Department of Financial Service cybersecurity compliance requirements (23 NYCRR 500)	https://www.governor.ny.gov/sites/default/files/atoms/files/Cybersecurity_Requirements_Financial_Services_23NYCRR500.pdf
Bank of England's "impact tolerance" for regulated firms and CBEST models	Bank of England et al., Operational Resilience: Impact Tolerances for Important Business Services (March 2022), available at: https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2021/ss121-march-22.pdf. Information on CBEST is available at: https://www.bankofengland.co.uk/financial-stability/operational-resilience-of-the-financial-sector/cbest-threat-intelligence-led-assessments-implementation-guide.

[1] All citations listed in this table last accessed on Sept. 19, 2022.
[2] The CFATS Risk-Based Performance Standard (RBPS) 8 addresses cybersecurity.

II. Discussion of the Advance Notice of Proposed Rulemaking

In light of the critical role that pipelines and rail sectors play in our Nation's economic and national security, as well as the ongoing and growing cyber threats to such sectors, TSA has determined that it is appropriate to issue a regulation for CRM in these sectors. This ANPRM is the first step in this process.

A. Policy priorities

TSA is issuing this ANPRM to solicit input to ensure this rulemaking effort adequately addresses the following policy priorities:

- *Assessing and improving the current baseline of operational resilience and incident response*. Prevention alone is not sufficient. An effective CRM program and regulatory regime must be based on the assumption that cyber-attacks will disrupt individual systems and processes that support important business services. Improving the capacity and ability to respond and recover swiftly when a cybersecurity incident occurs is key to mitigating disruption and ensuring resilient operations in today's cyber threat environment.
- *Maximizing the ability for owner/operators to be self-adaptive to meet evolving threats and technologies.* Traditionally, regulations prescribe generally static requirements, *i.e*., particular control or performance requirements that endure until the regulator issues a modification. To ensure that cybersecurity requirements sustain their effectiveness, regulations should provide for a continuous assessment of the current threat environment and ensure timely adaptation of dynamic security controls based on identified tactics, techniques, and procedures of malicious cyber actors and adversaries, while at the same time allowing for implementation of emerging technologies and capabilities that provide security controls that may be more relevant and effective for their intended purpose.
- *Identifying opportunities for third-party experts to support compliance.* The use of third-party evaluators and certifiers of cybersecurity programs and

cloud service providers can drive sustainable compliance at a scale that exceeds TSA's compliance resources.

- *Accounting for the differentiated cybersecurity maturity across the surface sector and regulated owner/operators.* Surface sub-sectors and owner/operators have varying degrees of capability and capacity to adopt cybersecurity standards. A regulatory regime that drives improvement to baseline thresholds and fosters resilience of the sector, even as adversaries adapt to target the weakest link, should, to the extent possible, leverage a maturity-based model to ensure required controls are commensurate with cyber risk.
- *Incentivizing cybersecurity adoption and compliance.* An effective regulatory regime is one that incentivizes and facilitates adoption and ensures that different components of the regime are reinforcing one another. While subsidies and grants may be the first incentives that come to mind, they also require a funding source that is beyond TSA's control.
- *Measurable outcomes.* To the greatest extent possible, quantifiable measures to assess performance should be built into a cybersecurity regulatory regime. Regulations should recognize the need for identifying expected performance outcomes up front, and then adjusting these measures over time through an iterative process that reflects the current operations, including organizational issues, IT and OT systems, and known cybersecurity risks.
- *Regulatory Harmonization.* TSA recognizes the importance of ensuring that cybersecurity requirements are risk-informed, outcome/performance-based

rules and, to the extent practicable, are consistent and harmonized with other applicable cybersecurity regulatory requirements.

B. Core elements of cybersecurity risk management

Following a review of the standards and guidelines identified above, and others, TSA identified common core elements of effective CRM. In discussions with subject matter experts, TSA also identified areas where additional requirements not captured in many current regimes are needed. Together, TSA believes that the following core elements would provide a bedrock of CRM for the pipeline and rail sectors.

- Designation of a responsible individual for cybersecurity;
- Access controls;
- Vulnerability assessments;
- Specific measures to gauge the implementation, effectiveness, efficiency, and impact of cybersecurity controls;
- Drills and exercises;
- Technical security controls (*e.g.,* multi-factor authentication, encryption, network segmentation, anti-virus/anti-malware scanning, patching, and transition to "zero trust" architecture);
- Physical security controls;
- Incident response plan and operational resilience;
- Incident reporting and information sharing;
- Personnel training and awareness;
- Supply chain/third-party risk management; and
- Recordkeeping and documentation.

C. Request for input to inform rulemaking

TSA requests constructive input on current cybersecurity practices that reflect an understanding of both cybersecurity and the operational issues of applying CRM to pipeline and rail operations. As noted above, TSA is specifically interested in comments from the applicable owner/operators, their representative associations, labor unions, state, tribal, and local governments, and the general public who rely on these systems.

In addition to input on CRM and general operational issues, TSA is interested in understanding cost implications. Such input on costs is critical for understanding the potential impacts of a regulation, and specifically to inform proper accounting of associated costs and benefits.

For those pipeline and rail owner/operators subject to the requirements in recently issued security directives imposing cybersecurity requirements, we are not expecting re-submission of information that has already been provided to TSA pursuant to the security directives, such as information contained in the results of cybersecurity vulnerability assessments.

TSA believes that cybersecurity regulations should consider current voluntarily-implemented cybersecurity measures and related operational issues that affect implementation of these measures. Having a clear and comprehensive understanding of the current baseline will support TSA's efforts to provide more flexibility in meeting the desired security outcomes. To that end, TSA is seeking specific information, including information about the costs and additional staffing requirements associated with past cybersecurity-related efforts, to assist in developing effective regulatory policies, resources for implementation, and valid cost estimates.

As discussed below, TSA is aware of the diversity of surface transportation operations, including national-level companies, publicly-owned systems, and small businesses, and of the need to ensure that requirements do not have unintended consequences on operations. To ensure that regulatory requirements reflect this concern, TSA asks commenters to include information regarding the nature and size of their business, as well as any information that could help TSA avoid regulations that have the potential to result in preventable operational impacts. This information will help TSA better understand and analyze the information provided. Failure to include this specific information will not preclude the agency's consideration of the information submitted.

III. Specific Requests for Comments

A. Overview

Responses to the following questions will help TSA develop a more complete and carefully considered rulemaking or appropriate next step. The questions are not all-inclusive, and any supplemental information is welcome. In responding to each question, please explain the reasons for your answer. We encourage you to let us know your specific concerns with respect to any of the topics under consideration.

As noted above, input received from this ANPRM will allow TSA to better understand how the pipeline and rail sectors are implementing CRM in policies, planning, and operations, and assess the need to update existing or develop new regulations to address CRM. TSA may share this information with other U.S. Government agencies to help develop future policies, guidance, and regulations on cybersecurity in the pipeline and rail sectors.

TSA recognizes that the phrase "cyber risk management" may involve a wide range of applications related to cyber safety and security. We request relevant information on all issues and challenges related to CRM development and implementation for pipeline and rail owner/operators in the areas of the standards, regulatory barriers, economic burdens, training and education, and management and oversight.

If you note in your submission that the information you are providing is business confidential, proprietary, or SSI, we will not share it with the public to the extent allowed by law. TSA may consider this information, however, to inform policy decisions or cost estimates in developing a proposed rule regarding CRM.

When considering your comments and suggestions, we ask that you keep in mind TSA's mission to protect the nation's transportation systems to ensure freedom of movement for people and commerce and protect our national and economic security. Commenters should feel free to answer as many questions as desired, but please consider the principles below in responding. Whenever appropriate, commenters should provide the following as part of their responses:

- If the comment refers to a specific program, regulation, guidance, standard, or policy at issue, please provide a specific citations and a link to the relevant document, as applicable;
- If the comment raises specific concerns about application of an existing program, regulation, or policy, please provide specific suggestions that identify alternative way(s) for the agency to achieve its regulatory objectives; and

- Provide specific data that documents the costs, burdens, and benefits described in the comment submission.

B. Identifying current baseline of operational resilience and incident response

B.1. What cybersecurity measures does your organization currently maintain and what measures has your organization taken in the last 12 months to adapt your cybersecurity program to address the latest technologies and evolving cybersecurity threats? What are your plans to update your cybersecurity program in the next 12 months? How much does your organization spend on cybersecurity annually?

B.2. What assessments does your organization conduct to monitor and enhance cybersecurity (such as cybersecurity risk, vulnerability, and/or architecture design assessments, or any other type of assessment to information systems)? How often are they conducted? Who in your organization conducts and oversees them? What are the assessment components, and how are the results documented?

B.3. Do the assessments you discussed in your response to B.2. use specific cybersecurity metrics to measure security effectiveness? If so, please provide information on the metrics that you use.

B.4. Are the actions you discussed in response to question B.1. based on any of the standards identified in section I.H. of this ANPRM? If so, please specify which standard. If your response is based on standards not identified in section I.H. of this ANPRM, please identify the standard and provide a link or other information to assist TSA in gaining a better understanding of the scope and benefits of the standard.

B.5. For any standards identified in response to question B.3.:

a. Are there fees associated with accessing copies of these standards?

b. Have you found these standards to be effective against cyber related threats? If your answer is no, please explain why.

c. Please provide any information on costs and benefits, if any, associated with implementing the standards.

d. Is adoption of these standards, or other cybersecurity measures, required or incentivized by insurance companies, existing commercial contracts, or contracts with the Federal Government? Please also provide any information on other incentives to encourage adoption of these or other standards.

B.6. "Operational technology" is a general term that encompasses several types of control systems, including ICS, SCADA, 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. If your OT systems are connected to an outside network (satellite, hardline internet, port wide computer network, *etc*.), what safeguards are you using to protect them from cyber threats? What are the costs to implement and maintain these safeguards? In addition, please provide details on cyber related standards or guidelines being used to guide actions assessing and mitigating threats to installed OT systems connected to vital operational equipment.

C. Identifying how CRM is implemented

The following questions apply to pipeline and rail owner/operators that have implemented CRM.

C.1. Please describe how your organization has implemented or plans to implement CRM. What frameworks, standards, or guidelines have informed your implementation of CRM for your pipeline and rail operations? Would you recommend any other standards or guidelines not mentioned in this ANPRM for application to pipeline or rail CRM programs? If possible, please provide any data available on the overall average cost to initially implement an owner/operator CRM and its annual costs to maintain (even if not a single action).

C.2. Does your CRM include aspects of system protection, system penetration testing, security monitoring, incident response, incident forensic analysis, and a plan for restoration of operations? If not, which features does your CRM address? What are the challenges for incorporating any missing facets? Are some parts of CRM developed in-house while a third-party develops other pieces? If so, why and what advantages do either of these approaches offer?

C.3. Does your CRM include any other core elements identified in Section II.B. or other measures not previously discussed? Are some aspects developed in-house while a third-party develops other facets? If so, why and what advantages do either of these approaches offer?

C.4. As part of implementing CRM, has your company developed or does it anticipate developing and maintaining CRM using in-house or newly acquired staff, or do you currently contract out developing and maintaining ongoing CRM to a third-party contractor or plan to do so? If your company uses a third-party or contractor to perform

this function, please explain why. In addition, if you use a third-party contractor, do you have a vendor management program or framework in place? Do you have a vendor integrity audit program to ensure vendors are legitimate and have additional security measures, such as an insider threat program? Does your vendor also provide penetration testing? If CRM is or will be developed and managed in-house, what is the expected annual cost in terms of wage and hours of development and management? If CRM is or will be contracted out, what are the retainer and associated fees for the third-party? Do annual fees increase by the number of incidents they respond to and, if so, by how much?

C.5. What cybersecurity personnel training and security awareness and skills education should pipeline and rail owner/operators be required to provide, and to which employees (*i.e.*, should it apply to all employees or just those with specific responsibilities, such as cybersecurity personnel, those with access to certain systems, *etc*.)? Please provide relevant information regarding what CRM training courses are available and the duration of each course, as well as how much it costs you to develop and conduct or otherwise provide CRM training and update current courses and training requirements. This information should include costs for owner/operators to create or procure course content for the types of employees identified.

C.6. How does your company address, respond to, or modify business practices due to the cost impacts of a cybersecurity incident? Does your company maintain estimates of the cost impacts (with respect to your organization and external parties) of various types of cybersecurity incidents, including but not limited to ransomware, data breaches, and attacks on operational technology? If so, what is the range of these costs based on the type or severity of the incident? Does your company insure against these

kinds of costs, and, if so, what is the annual cost of insurance, and what kind of coverage is offered? If your company does not have insurance coverage, please explain why.

D. Maximizing the ability for owner/operators to meet evolving threats and technologies

D.1. In addition to the requirement to report cybersecurity incidents, should pipeline and rail owner/operators be required to make attempts to recover stolen information or restore information systems within a specific timeframe? If so, what would be an appropriate timeframe?

D.2. From a regulatory perspective, TSA is most interested in actions that could be taken to protect pipeline and rail systems by ensuring appropriate safeguards of critical cyber systems within IT and OT systems. What types of critical cyber systems do you recommend that regulations address and what would be the impact if the scope included systems that directly connect with these critical cyber systems? Please provide sufficient details to allow TSA to identify where and how your recommendations relate to our current requirements or recommendations, as discussed in Section I.E.

D.3. Recognizing that there are both evolving threats and emerging capabilities to address known threats, how could owner/operators adjust their vulnerability assessments and capabilities if TSA were to issue periodic benchmarks to pipeline and rail owner/operators on the scope of vulnerability assessments that are informed by the latest technologies and evolving threats? The purpose of the periodic guidance and assessments would be to facilitate the owner/operator's evaluation of vulnerabilities and capabilities based on the most current technologies and threats.

D.4. What are some benefits and challenges for pipeline and rail owner/operators in building operational resilience by conducting the vulnerability assessments required/recommended by TSA (whether based on the directives and information circulars discussed in Section I.E. of this ANPRM or the guidelines and assessments discussed in Section I.H.) and any assessments offered by CISA?[50]

D.5. What would be the benefits and challenges for the pipeline and rail sectors if owner/operators were required to use an accredited third-party certifier to conduct audits/assessments to determine effectiveness of the owner/operator's cybersecurity measures and/or compliance with existing requirements? What would be the costs of implementing a requirement to use a third-party certifier?

D.6. What impacts (positive and negative) to the pipeline and rail sectors workforce do you anticipate regarding the implementation of CRM? Will there be a need to hire additional employees? If so, how many and at what level and occupation?

D.7. Should pipeline and rail owner/operators be required to conduct third-party penetration testing to identify weakness or gaps in CRM programs? Please address the identified costs and benefits of this action, and any legal, security, privacy, or other issues and concerns that may arise during the testing process or prevent third-party penetration testing.

D.8. How could TSA maximize implementation of CRM by providing for innovative, effective, and efficient ways to measure cybersecurity performance? Please provide specific references or resources available for any measurement options discussed, as available.

---

[50] Source: CISA Assessments: Cyber Resilience Review (CRR), accessible at https://www.cisa.gov/uscert/resources/assessments

D.9. Should pipeline and rail owner/operators designate a single individual (such as a chief information security officer) with overall authority and responsibility for leading and managing implementation of the CRM? Or should they designate a group of individuals as responsible for implementation or parts thereof?

D.10. Should the individuals who you identified under D.8. be required to have certain qualifications or experience related to cybersecurity, and if so, what type of qualifications or experience should be required? If not, what specific requirements should there be for who would implement a pipeline and rail owner/operators' CRM program? Would implementing this type of requirement necessitate hiring additional staff? If so, how many and at what level and occupation?

D.11. Should pipeline and rail owner/operators be required to monitor and limit the access that individuals have to OT and IT systems in order to protect information and restrict access to those who have a demonstrated need for access to information and/or control? Actions include limiting user access privileges to control systems to individuals with a demonstrated need-to-know and using processes and tools to create, assign, manage, and revoke access credentials for user, administrator, and service accounts for enterprise assets and software. What would be the cost of implementing this type of requirement?

D.12. What CRM security controls should pipeline and rail owner/operators be required to maintain, and in what manner? Please address each of the following:

a. Defense-in-depth strategies (including physical and logical security controls);

b. Network segmentation;

c. Separation of IT and OT systems;

d. Multi-factor authentication;

e. Encrypting sensitive data both in transit over external networks and at rest;

f. Operating antivirus and anti-malware programs;

g. Testing and applying security patches and updates within a set timeframe for IT and OT systems; and

h. Implementing, integrating, and validating zero-trust policies and architecture.

D.13. Please provide information on the cost to implement and integrate the CRM security controls identified in your response to question D.12.

D.14. What baseline level of physical security of CRM architecture should pipeline and rail owner/operators be required to maintain, including ensuring that physical access to systems, facilities, equipment, and other infrastructure assets is limited to authorized users and secured against risks associated with the physical environment? How much would it cost to implement the baseline physical security measures you identified in your response? How many of the identified measures are currently maintained (if such information has not already been provided to TSA)?

D.15. What would the benefits and challenges be for pipeline or rail owner/operators to build operational resilience by adopting an "impact tolerance" framework to help ensure that important business services remain operational after a cybersecurity incident, as provided for in the Bank of England's *Operational Resilience: Impact Tolerances for Important Business Services*?[51]

D.16. What minimum cybersecurity practices should pipeline and rail owner/operators require that their third-party service providers meet in order to do

[51] *See, supra,* Table 1.

business with pipeline and rail owner/operators? What due diligence with respect to cybersecurity is involved in selecting a third-party provider? For example, do pipeline and rail owner/operators include contractual provisions that specifically require third-party service providers to maintain an adequate CRM program? Should TSA require such provisions, and if so, for what pipeline and rail segments and under what circumstances?

D.17. How can pipeline and rail owner/operators develop a process to evaluate service providers who hold sensitive data, or are responsible for enterprise critical IT platforms or processes, to ensure that these providers are protecting those platforms and data appropriately?

D.18. Please address the extent to which pipeline and rail owner/operators should ensure that processes to procure control systems include physical security and cybersecurity in acquisition decisions and contract arrangements? In addition, please address the extent to which pipeline and rail owner/operators should ensure that vendors in the supply chain are vetted appropriately and that vendors vet their own personnel, service providers, and products and software.

D.19. Are there any new technologies in use or under development that may be relevant to the future of secure IT and OT systems, and how should these technologies be considered or used to establish an effective regulatory CRM regime?

D.20. How should pipeline and rail owner/operators address cybersecurity challenges or benefits posed by using a commercial cloud service provider? Please explain how pipeline and rail owner/operators can identify and mitigate risks associated with migration of data, services, or infrastructure to a public or shared cloud storage

system and/or perspective on the security benefits and challenges that may arise from the use of commercial cloud infrastructure.

D.21. How can pipeline and rail owner/operators most effectively address the risks of using very small aperture terminals networks and commercial satellite communications for remote communications? Please address how pipeline and rail owner/operators can identify and mitigate risks associated with use of these systems, which were often built for speed of communication without security in mind or specific measures to address known vulnerabilities. What would be the cost of implementing the actions you recommend for identifying and mitigating risks associated with these systems? If cost data are provided, please break it down by unit and extent to which they are implemented (*e.g.*, isolated or system-wide).

D.22. What other regulatory or procurement regimes do pipeline and rail owners/operators need to comply with (*e.g.,* are you required to comply with Defense Federal Acquisition Regulation Supplement (DFARS) requirements)? What actions/documentation can pipeline and rail owner/operators take/provide to allow TSA to consider compliance with another state or federal requirement to establish full compliance with TSA's requirements? How could TSA validate that the other requirements are, in fact, being fully implemented and provide the same level of security as TSA's requirements? Are there other regulatory regimes, potentially in other sectors or other countries, that pipeline and rail owners/operators believe would be good references for TSA?

D.23. How can maturity-based cybersecurity frameworks, such as CISA's Cross-Sector Cybersecurity Performance Goals and the *NIST Framework for Improving Critical*

Infrastructure Cybersecurity,[52] be leveraged in the pipeline and rail sectors to calibrate adoption in a manner that is tailored and feasible for these sectors?

D.24. What existing statutes, standards, or TSA-issued regulations, policies, or guidance documents may present a challenge or barrier to the implementation of CRM in the pipeline and rail sectors? How could these statutes, standards, regulations, policies, or guidance documents be changed to remove the barriers or challenges? Please be as detailed and specific as possible.

D.25. How could a future rulemaking implement risk-based and/or performance based requirements that achieve an effective cybersecurity baseline across the pipeline and rail industry?

E. Identifying opportunities for third-party experts to support compliance

The following questions are specifically related to the role of third-parties to establish compliance with requirements, such as verifications and validations. TSA has maximized the capability of third-party certifiers in other contexts and is interested in options for leveraging this capability for cybersecurity. In general, the concept would require some level of approval by the Federal Government that recognizes the qualifications of the third-parties, vetting to identify any potential conflicts of interest or other risks associated with an insider threat, and consistent standards to be applied.

E.1. How would you envision using third-party organizations to improve cyber safety and security in the pipeline and rail sectors? For example, should pipeline and rail owner/operators be able to use third parties to administer their CRM programs, and if so, to what extent and in what manner? Should pipeline and rail owner/operators use third-

[52] *See* Table 1.

party certifiers to verify compliance and the adequacy of their CRM programs? Please explain the basis for your position and provide specific examples and, where possible, estimated costs.

E.2. What would the benefits and challenges be were TSA to require owner/operators to conduct compliance assessments by an accredited third-party certifier, similar to that described in the Bank of England's *CBEST Threat Intelligence-Led Assessments* (2021)? What features should be included in a compliance scheme that leverages third-party validators?

E.3. What minimum cybersecurity practices or experience should TSA require that third-party experts meet for them to do business with the pipeline and rail owner/operators?

F. Cybersecurity maturity considerations

F.1. What special considerations or potential impacts (*i.e.,* risks, costs, or practical limitations) would pipeline and rail owner/operators have to consider before implementing CRM in their respective operations? Are there differences between startup costs to implement and the ongoing costs to maintain CRM? Do small entities (including business owner/operators) face unique or disproportionate costs in implementing and maintaining CRM?

F.2. What is your estimate of the percentage of pipeline and rail owner/operators that have already implemented CRM within their organizations? If you do not know specifically, please provide us with your best estimate or any sources of data that TSA may use to determine this number. Does your organization currently have a CRM

program? Do you think there are disparities between the percentages of large and small entities that have implemented CRM? If so, why and what are they?

F.3. Some sectors may have regulatory regimes in place imposing cybersecurity requirements. As some owner/operators may be subject to regulatory requirements imposed by multiple Federal, state, or local agencies, how should TSA most effectively achieve regulatory harmonization consistent with our transportation security responsibilities and relevant to pipeline and rail owner/operators?

G. Incentivizing cybersecurity adoption and compliance

TSA is particularly interested in comments on types of incentives, such as liability protection, insurance, commercial contracts, or other private or public sector options, that would incentivize adoption of cybersecurity and resilience measures, and whether and how TSA might facilitate the development of such incentives.

G.1. If you have implemented CRM, was implementation required or incentivized by insurance companies, existing commercial contracts, or contracts with the Federal Government? How long did it take to implement CRM and what was the estimated cost of the implementation? What are the estimated annual costs of maintaining your CRM program?

G.2. Does your company insure against significant cybersecurity incidents? If so, what are the general terms of your insurance, and how does it factor into your decision on how to respond to significant cybersecurity incidents? What is the scope of review or audits that your insurer conducts, or requires you to conduct, in order to assess insurance worthiness?

G.3. What tools, technical assistance, or other resources could TSA provide to facilitate compliance with any specific federally-imposed cybersecurity requirement?

Dated: November 22, 2022.

David P. Pekoske,

Administrator.

[FR Doc. 2022-25941 Filed: 11/29/2022 8:45 am; Publication Date: 11/30/2022]