1. ***Explain the circumstances that make the collection of information necessary. Identify any legal or administrative requirements that necessitate the collection. Attach a copy of the appropriate section of each statute and regulation mandating or authorizing the collection of information. (Annotate the CFR parts/sections affected).***

The Transportation Security Administration (TSA) has broad authority with respect to transportation security and supported with specific powers related to the development and enforcement of regulations and other requirements. For example, under the Aviation and Transportation Security Act (ATSA)[1] and delegated authority from the Secretary of Homeland Security, TSA has broad responsibility and authority for "security in all modes of transportation . . . including security responsibilities . . . over modes of transportation that are exercised by the Department of Transportation."[2] In addition, the Implementing Recommendations of the 9/11 Commission Act (9/11 Act)[3] requires regulations for higher-risk public transportation agencies, railroads, and Over-the-Road Bus (OTRB) owner/operators to develop security plans to address specific security issues and vulnerabilities identified during an assessment of specific systems, infrastructure, and capabilities.[4]

[1] Pub. L. 107-71; 115 Stat. 597 (Nov. 19, 2001).
[2] 49 U.S.C. 114(d).
[3] Pub. L. 110-53 (121 Stat. 266; Aug. 3, 2007).
[4] *See* secs. 1405 and 1512 of the 9/11 Act, as codified at 6 U.S.C. 1134 and 1162, respectively; *see also* section 1531, as codified at 6 U.S.C. 1181 (which imposes similar requirements for OTRBs).

TSA has previously imposed requirements to address cybersecurity risks to transportation security through Security Directives (SDs) issued under the emergency authorities provided to TSA under ATSA, specifically 49 U.S.C. 114(*l*)(2).[5] TSA's Enhancing Surface Cyber Risk Management (CRM) Notice of Proposed Rulemaking (NPRM) codifies the cybersecurity requirements in these SDs along with additional requirements, and reorganized these requirements to align with the Cross-Sector Cybersecurity Performance Goals (CPGs) developed by the Cybersecurity Infrastructure and Security Agency (CISA)[6]. The CRM NPRM addresses the pervasive cybersecurity threats to the Nation's most critical pipeline, freight, and public transportation and passenger rail infrastructure.

The requirements proposed by TSA through the CRM NPRM would strengthen cybersecurity and resiliency for the surface transportation sector by mandating reporting of cybersecurity incidents and development of a robust CRM program. This rulemaking builds upon TSA's previously issued requirements and recommendations, the cybersecurity framework developed by the National Institute of Standards and Technology (NIST), and CISA's CPGs.

The NPRM proposes to require owner/operators of designated freight railroads, passenger railroads, rail transit, and pipeline facilities and/or systems to have a CRM program approved by TSA. The proposed CRM program includes three primary elements. First, owner/operators to whom the rule applies 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.

[5] *See* SD Pipeline-2021-01 Series - Enhancing Pipeline Cybersecurity; SD Pipeline-2021-02 Series - Pipeline Cybersecurity Mitigation Actions, Contingency Planning, and Testing; SD-1580-21-01 Series - Enhancing Rail Cybersecurity; SD-1582-21-01 Series - Enhancing Public Transportation and Passenger Railroad Cybersecurity; and SD-1580/82-2022-01 Series - Rail Cybersecurity Mitigation Actions and Testing. Each of these documents is available at: https://www.tsa.gov/sd-and-ea.

[6] CISA's Cybersecurity Performance Goals (CPGs) are a subset of cybersecurity practices, selected through a thorough process of industry, government, and expert consultation, aimed at meaningfully reducing risks to both critical infrastructure operations and the American people. More information is available on CISA's website for

.

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

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

As part of this rule, TSA also is proposing to reorganize requirements in subchapter D of 49 CFR chapter XII related to security coordinators, reporting significant security, and security training of security-sensitive employees. TSA would move these requirements from 49 CFR part 1570[7] and add them to the specific modal requirements in parts 1580, 1582, 1584[8], and the new part 1586, which is applicable to pipeline systems and facilities.

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

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

While the requirements in this proposed rule would not address all elements of vulnerability assessments and security plans stipulated in the 9/11 Act, it would address the 9/11 Act's requirements as they relate to the information and operational technology systems used by high-risk freight railroads and PTPR systems. For example, the 9/11 Act requires

[7] Surface transportation modes required to have a Security Program.
[8] Freight railroads, public transportation and passenger railroads, and Over-the-Road Buses.

identification and evaluation of critical systems, including information systems,[9] plans for providing redundant and backup systems needed to ensure continued operations in the event of a cybersecurity incident, and identification of the vulnerabilities to these systems.[10] The vulnerability assessment applicable to higher-risk rail carriers must also identify strengths and weaknesses in (1) 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.[11] For security plans, the statute requires regulations that address, among other things, actions to mitigate identified vulnerabilities, the protection of passenger communication systems, emergency response, ensuring redundant and backup systems are in place to ensure continued operation of critical elements of the system in the event of a terrorist attack or other incident, and other actions or procedures as the Secretary determines are appropriate to address the security of the public transportation system or the security of railroad carriers, as appropriate.[12] The provisions proposed in this NPRM would satisfy such requirements as they relate to cybersecurity in high-risk public transportation agencies and railroads.

The Office of Management and Budget (OMB) has currently approved information collections associated with cybersecurity SD requirements.[13] Both DHS and TSA have publicly indicated the intent for TSA to codify the requirements issued through SDs to pipeline and rail owner/operators through notice and comment rulemaking.[14] On October 6, 2021, Secretary Mayorkas announced that TSA would initiate a rulemaking process "to develop a longer-term regime to strengthen cybersecurity and resilience in the transportation sector."[15]

This proposed collection consolidates and replaces all current ICR requirements for CRM of freight rail, passenger rail, and pipeline owner/operators under one OMB control number.

---

[9] *See* secs. 1405(a)(3) and 1512(d)(1)(A) of the 9/11 Act, as codified at 6 U.S.C. 1134(a)(3), 1162(d)(1)(A), respectively.

[10] *See id.* at secs. 1405(c)(2), 1512(d)(1)(D), and 1512(e)(1)(G), as codified at 6 U.S.C. 1134(c)(2), 1162(d)(1)(D), 1162(e)(1)(G), respectively.

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

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

[13] For Pipeline see 1652-0050, 1652-0055 and 1652-0056. For Freight Rail, see 1652-0074. For passenger rail, see 1652-0074. Available at Search of Information Collection Review (reginfo.gov)

[14] The Enhancing Surface Cyber Risk Management rulemaking is listed in the OMB Spring 2023 Unified Agenda of Regulatory and Deregulatory Actions. Available at Current Unified Agenda of Regulatory and Deregulatory Actions (reginfo.gov).

[15] A copy of the Secretary's remarks is available at: https://www.dhs.gov/news/2021/10/06/secretary-mayorkas-delivers-remarks-12th-annual-billington-cybersecurity-summit.

Upon approval of the new ICR and publication of a final rule, TSA will amend, or as appropriate rescind, the current ICRs associated with TSA SDs currently in effect.

2. Indicate how, by whom, and for what purpose the information is to be used. Except for a new collection, indicate the actual use the agency has made of the information received from the current collection.

Even though most of the ICRs in the CRM NPRM are currently covered by approved ICRs, TSA is adding a few new requirements requiring information collection that were not previously included in TSA SDs or otherwise in approved ICRs. TSA's objective in this cybersecurity rulemaking is to make CRM requirements comprehensive and forward-looking.

These new requirements for all rail (freight, passenger, and transit) and pipeline owner/operators subject to the ICR include: (1) submission of a Cybersecurity training program to TSA for approval (reporting); (2) maintaining records of employee cybersecurity training (record keeping); and, (3) maintaining records of inclusion of supply chain security measures in the owner/operator's Cybersecurity Operational Implementation Plan (COIP). OTRB owner/operators are currently required to report significant security concerns and would also be required to report cybersecurity incidents.

Finally, the CRM NPRM proposes to add a new requirement for pipeline owner/operators to: (1) designate a physical security coordinator and submit the contact information to TSA and (2) report significant physical security concerns to TSA. This additional requirement for pipelines would align with requirements applicable to the other owner/operators covered by the proposed rule. Upon finalization of the CRM rulemaking, TSA will use the information collection to establish compliance with the new regulatory requirements. By implementing these performance-based requirements, TSA would ensure that the 293 higher-risk entities have measures in place to address current cybersecurity risks with the flexibility necessary to address emerging threats and deploy evolving capabilities, and that CISA and TSA are receiving information on cybersecurity threats from all higher-risk surface owner/operators identified by TSA, including 71 OTRB entities not currently subject to the SDs.

Specifically, the information collection requirements for the CRM NPRM would apply to:

- 73 freight railroads that transport the greatest amount of cargo or are identified as supporting certain Department of Defense operations.
- 34 rail transit and passenger railroads including Amtrak, with the largest daily ridership, based on both location and passenger volume as primary risk considerations.
- 115 hazardous liquids, natural gas, and liquefied natural gas pipeline systems and facilities that transport the largest volume of these commodities. A successful cyber-attack on these systems could lead to a sustained disruption in service and affect their necessary capacity to support national and economic security needs.
- 71 OTRB entities due to their fixed-route passenger service through designated Higher-Threat-Urban Areas; OTRB entities would only be subject to the proposed requirement for reporting cybersecurity incidents to CISA.

The following table provides an explanation of the purpose/benefit for each information collection requirement in the CRM NPRM (an "*" indicates a proposed requirement not currently covered by other OMB control numbers).

Table 1: Proposed CRM Requirements Purpose and Benefits

CRM Requirement	Summary of Requirement	Purpose / Benefit
Conduct an enterprise-wide Cybersecurity Evaluation (CSE) - 1580.305, 1582.205, and 1586.205	Record keeping. Owner/operators would be required to maintain documentation of the completion of an annual CSE; which must be made available to TSA upon request. The CSE must be sufficient to determine the owner/operator's current enterprise-wide cybersecurity profile of logical/virtual and physical security controls and assess their current cybersecurity posture consistent with the target profile established through this rulemaking.	The evaluation will identify security vulnerabilities and strengths by looking at the issue of cybersecurity enterprise wide. For example, this type of assessment helps owner/operators identify areas where safeguards are weak, but may also help identify areas where compensating controls are provided through physical or other defense-in-depth policies and measures. Furthermore, understanding and monitoring an organization's cybersecurity profile over time through recurrent evaluations provides benefit by focusing attention on cybersecurity, providing a means to evaluate cyber-related threats and mitigation measures put in place, prioritizing responses and investments to address threats and vulnerabilities where they will have the most effect, and informing budgeting for upgrade cycles and longer-term investments.
Develop and obtain TSA approval of a COIP – 1580.307, 1582.207, and 1586.207	Reporting. Owner/operators would be required to develop and submit for TSA approval a COIP that meets the security outcomes specified in the rule. This plan aligns with the existing requirements for a Cybersecurity Implementation Plan (CIP) required by the SD Pipeline-2021-02 and SD 1580/82-21-02 series. The COIP must include specific detail on exactly how the owner/operator meets the requirements for (a) governance; (b) identification of Critical Cyber Systems (CCS), network architecture, and interdependencies; (c) procedures, policies, and capabilities to protect CCSs; and (d) procedures, policies, and capabilities to detect cybersecurity incidents. The COIP must include a Plan of Action and Milestones (POAM) that identifies a schedule for the specific measures to be implemented, within 3 years, to meet all required outcomes, and any measures in place to mitigate the risks associated with not fully complying with the requirements or security outcomes.	The COIP is the owner/operator's plan to meet specific cybersecurity outcomes as required in the rule. Once approved, the COIP is a TSA-approved security program and becomes the basis for TSA compliance inspections. The COIP is flexible, allowing the owner/operator to determine how they will meet specific cybersecurity outcomes, for example access control, while providing TSA the means to measure compliance. 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. Including a POAM in the CIP ensures that a written plan is in place to meet the cybersecurity outcomes specified in the rule. The POAM would allow an owner/operator who cannot immediately meet a specific requirement to have a measurable timeline, subject to compliance, for meeting the requirement. The potential vulnerability resulting from the delay in achieving full compliance must be offset by effective, temporary alternative measures sufficient to mitigate the cybersecurity vulnerability.
*Designate an Accountable Executive for CRM Program – 1580.309(a), 1582.209(a), and 1586.209(a)	Reporting. Owner/operators would be required to designate an accountable executive for their CRM program in their COIP and provide that information to TSA. The information collection would include the names, titles, business telephone numbers, and business email addresses. The accountable executive is the primary individual to be contacted with regard to the owner/operator's CRM program.	Identification of an accountable executive provides authority, legitimacy, and a central point of contact for the owner/operator's CRM program. An accountable executive helps ensure owner/operators have a clear line of authority from which to pursue strategic objectives, align cybersecurity policy to applicable Federal standards, and manage and oversee execution of the CRM program.
Designate a Cybersecurity Coordinator – 1580.311, 1582.211, and 1586.211	Reporting. Owner/operators would be required to appoint a Primary and Alternate Cybersecurity Coordinator and submit their contact information to TSA. The Cybersecurity Coordinator, or alternate, serves as the primary contact for cyber-related intelligence information and cybersecurity-related activities and	TSA has found significant value in having an owner/operator point of contact to address cybersecurity issues. Designating a primary and alternate Cybersecurity Coordinator ensures that TSA can swiftly engage with a central person to share emergent threat information, discuss needs and requirements, and provide information in

CRM Requirement	Summary of Requirement	Purpose / Benefit
	communications with TSA and CISA and must be accessible to TSA and CISA 24 hours a day, 7 days a week. The primary Cybersecurity Coordinator must be a U.S. citizen.	response to a cybersecurity incident.
*Develop and submit to TSA for approval a Cybersecurity Training Program and maintain cybersecurity training records – 1580.319, 1582.219, and 1586.219.	Reporting**.** Owner/operators would be required to develop and submit to TSA for approval a cybersecurity training program. The program would be required to meet the requirements specified in the rule. Record Keeping. Owner/operators would be required to maintain training records for all employees and contractors with access to owner/operator IT or OT systems demonstrating employee completion of basic cybersecurity training. Owner/operators would be required to maintain training records demonstrating completion of role-based cybersecurity training for individuals designated as cybersecurity-sensitive employees.	The prevention of cybersecurity incidents includes the awareness and knowledge of all employees on cyber-hygiene best practices, acceptable use, and cybersecurity risks. Owner/operators must have a cybersecurity training program in place for all employees as an essential cybersecurity prevention method. Annual cybersecurity training will strengthen cybersecurity knowledge among all employees, thus making them less susceptible to threats and more prepared to take action when threats occur. Additionally, those employees with increased level of access to sensitive systems require additional role-specific training to ensure they understand and are aware of their responsibilities regarding acceptable use and the risks associated with their level of access.
Report Cybersecurity Incidents to CISA – 1580.325, 1582.225, 1584.107, and 1586.225	Reporting. Owner/operators would be required to report cybersecurity incidents as defined in the TSA Cybersecurity Lexicon, to CISA within 24 hours of identification. Owner/operators may be requested to provide follow-up information to CISA (as needed). Cybersecurity incident reports are submitted using the CISA Reporting System form at: . Incident reports can also be reported by calling (888) 282-0870. This collection is covered by an OMB-approved CISA information collection for cybersecurity incident reporting. See OMB control number 1670-0037. TSA would require certain OTRB owner/operators to report cybersecurity incidents; but is not proposing to require OTRB owner/operators to develop and implement a full CRM program.	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 may shorten its recovery time. Other surface transportation owner/operators, and in turn the public, benefit from TSA and CISA knowing 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 may also use the reported incident to identify trends, assist in the response, and try to help mitigate any broader impacts to the larger economy.
Develop and Implement a Cybersecurity Incident Response Plan (CIRP) – 1580.327, 1582.227, and 1586.227	Record keeping. Owner/operators would be required to maintain documentation of a CIRP that addresses the security outcomes specified in the rule.	A comprehensive CIRP allows owner/operators to respond effectively to a cybersecurity incident and recover more quickly. It is essential that personnel have defined responsibilities, and the owner/operators have policies and procedures in place to respond to a cybersecurity incident. A CIRP would reduce the risk of operational disruption should their IT and/or OT systems be affected by a cybersecurity incident.
Develop and submit to TSA for approval a Cybersecurity Assessment Plan (CAP) that assesses effectiveness of cybersecurity measures in place and document this in a CAP annual report – 1580.329, 1582.229, 1586.229	Reporting (CAP). Owner/operators would be required to develop and submit to TSA for approval a CAP that meets the requirements specified in the rule.	An effective CRM program includes an assessment plan of the program. It is essential that a process is in place to: 1) ensure the right cybersecurity measures are in place and 2) that they are effective. A requirement to update the plan annually ensures that all elements of the CRM program are reviewed on a periodic basis. It also ensures that the plan considers evolving technology and threats.
Maintain documentation to establish compliance – 1580.331, 1582.231, and 1586.231 (Related to 1570.117)	Recordkeeping. TSA may request to inspect or copy documents to establish compliance as specified in the rule. Under proposed 1570.l17, a revision to current 1570.121, TSA would require maintenance of records sufficient to establish compliance and	The purpose of this section is to identify the types of documentation that could be used to establish compliance with the regulatory requirements. TSA is not requiring that these documents be maintained, but providing awareness of the types of documents the agency may ask to see as part of an inspection. Based on TSA's experience, not having

CRM Requirement	Summary of Requirement	Purpose / Benefit
	provide instructions on how to incorporate by reference critical documents into the security program.	these documents may make it difficult for an owner/operator to establish compliance. TSA is providing flexibility for owner/operators to use previously developed plans, procedures, policies, and other documents to be used to meet the proposed requirements. This flexibility, however, requires that these other documents be incorporated by reference into the COIP so that they become part of the program. Absent this step, TSA would not be able to approve the COIP as meeting the security program requirements in the proposed rule.
Designate a Physical Security Coordinator (Primary and Alternate) – 1580.103, 1582.103, 1584.103, and 1586.103	Reporting. Each owner/operator is required to designate and provide to TSA the contact information of a primary and at least one alternate Physical Security Coordinator. TSA is proposing to move the requirement in current 1570.201 to each modal section and expanding this requirement to pipeline facilities and systems. TSA is proposing to make designation of a Physical Security Coordinator mandatory for the pipeline owner/operators within the scope of applicability.[16] Adding this requirement for pipelines makes this requirement consistent with requirements for Freight Rail, PTPR, and higher-risk OTRB owner/operators, which are also required to have a Physical Security Coordinator.[17]	TSA has found significant value in having an owner/operator point of contact to address physical security issues. Designating a primary and alternate Physical Security Coordinator ensures that TSA can swiftly engage with a central person to share emergent threat information, discuss needs and requirements, and provide information in response to a significant physical security concern.
Report Significant Physical Security Concerns to TSA –1580.105, 1582.105, 1584.105[18], and 1586.105	Reporting. Each owner/operator is required to report Significant Physical Security Concerns to TSA. TSA is proposing a new requirement for the pipeline facilities and systems within the applicability of the CRM program to report significant physical security concerns. TSA is proposing to move the requirement in current 1570.203 to each modal section and expand this requirement to pipeline facilities and systems. Through this rulemaking, TSA is proposing to make reporting of significant physical security concerns mandatory for the pipeline owner/operators.[19] Adding this requirement for pipelines makes this requirement consistent for Freight Rail, PTPR, and higher-risk OTRB owner/operators, which are required to report significant physical security concerns to the TSA Transportation Security Operations Center within 24 hours of initial discovery.[20]	Reporting incidents to TSA allows TSA to share, as appropriate, threat information with other owner/operators for example on tactics, techniques, and procedures used in a breach of a facility. TSA would also use reported incidents to identify trends and identify specific vulnerabilities with regard to physical security measures. Regulated entities benefit from receiving feedback from TSA, so they can see the bigger picture and respond appropriately.

[16] Since 2010, TSA's Pipeline Security Guidelines have encouraged pipeline owner/operators to provide contact information for security operations or control centers for pipeline owner/operators in order to facilitate the exchange of information. See ICR 1652-0055.

[17] See OMB control number 1652-0066.

[18] TSA is also proposing to add Appendix B to 49 CFR part 1584, which would modify current Appendix A to part 1570 to be specifically applicable to OTRB entities.

[19] Since 2010, TSA's Pipeline Security Guidelines have encouraged pipeline owner/operators to report security incidents to TSA and provide contact information for security operations or controls centers for pipeline owner/operators in order to facilitate the exchange of information. See ICR 1652-0055.

[20] See OMB control number 1652-0066.

3. Describe whether, and to what extent, the collection of information involves the use of automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, e.g., permitting electronic submission of responses, and the basis for the decision for adopting this means of collection. Also describe any consideration of using information technology to reduce burden.

In compliance with the Government Paperwork Elimination Act, fully electronic reporting options are available for surface owner/operators as described below.

The Cybersecurity Coordinator contact information can be submitted to TSA via email or regular mail.

Cybersecurity incident reports are submitted using the CISA Reporting System form at: https://us-cert.cisa.gov/forms/report. Incident reports can also be reported by calling (888) 282-0870. This collection is covered by an OMB-approved CISA information collection for cybersecurity incident reporting. *See* OMB control number 1670-0037.

There are two options for owner/operators to make documents available to TSA for review and approval. These methods include submitting the required information, which is considered Sensitive Security Information (SSI) under 49 CFR part 1520 once completed, via a password protected email, or to upload the document via a specific secure portal that TSA has established using the Homeland Security Information Network (HSIN).

4. Describe efforts to identify duplication. Show specifically why any similar information already available cannot be used or modified for use for the purpose(s) described in Item 2 above.

DHS has a broad Memorandum of Understanding (MOU) with the Department of Transportation (DOT) that ensures coordination on security and safety issues. Through annexes to this MOU, TSA works closely with its partners at the Federal Railroad Administration, Federal Transit Administration, and Federal Motor Carrier Safety Administration to coordinate security initiatives. These annexes specifically address the respective roles and responsibilities of TSA and DOT as well as coordination processes across the sub-agencies. Due to the growing interdependence of critical systems that are of national and economic significance, TSA continued its coordination with the above federal agency partners that are critical to the cybersecurity posture of the surface transportation sector. TSA continued to consult with these Federal agency partners to develop the requirements and recommendations for the ICR associated with this NPRM.

In addition, TSA requires cybersecurity incident reports to be submitted using the CISA Reporting System form at: https://us-cert.cisa.gov/forms/report. Incident reports can also be reported by calling (888) 282-0870. This reporting requirement consolidates this information within CISA.

There is no other similar mandatory information collection currently in place at any Federal agency that specifically targets corporate-level cybersecurity planning and plan implementation in the surface modes of transportation.

5. If the collection of information has a significant impact on a substantial number of small businesses or other small entities (Item 5 of the Paperwork Reduction Act submission form), describe the methods used to minimize burden.

This collection of information impacts some small entities that have been deemed critical owner/operators in freight rail and pipeline transportation modes. The collection of information is necessary to ensure compliance with this requirement imposed to enhance the cybersecurity posture of the surface transportation modes and security, public safety, and property protection of interconnected critical infrastructure and the supply chain. There are no small PTPR entities[21] impacted by this rule, nor is there a significant impact to small OTRB entities.

TSA has strived to minimize the burden imposed on small businesses or other small entities from the time limits on collecting required information, while balancing the need to enhance surface transportation and national security. In an effort to reduce this time burden, TSA has implemented an alternative method to sending information solely by email, and can now securely collect all documentation electronically using the HSIN.

6. Describe the consequence to Federal program or policy activities if the collection is not conducted or is conducted less frequently, as well as any technical or legal obstacles to reducing burden.

If the information is not collected in the manner prescribed by the CRM NPRM, the lack of this information will hinder TSA's ability to assess physical and cybersecurity vulnerabilities and carry out requirements to protect the traveling public and secure Critical Control Systems and the Nation's surface transportation systems.

Cybersecurity Operational Implementation Plan (COIP). Without means of collecting this information, TSA would be unable to confidently ensure that entities are enhancing the cybersecurity posture of their Critical Cybersecurity Systems by reducing vulnerability to cybersecurity incidents and strengthening response measures in the event of a cybersecurity incident.

Cybersecurity Coordinator. TSA is responsible for sharing cyber-related intelligence and other risk information relevant to the transportation industry. Lack of cybersecurity coordinator information impedes TSA's ability to share information, potentially resulting in diminished capability for industry and the government to assess and respond to threats, incidents, and other security-related actions.

[21] TSA analyzed 34 PTPR owner/operators that would be affected by this proposed rule. TSA uses the Small Business Association size standards to identify that none of the PTPR owner/operators (of the 34) affected by the proposed rule are considered a small business. There are no small PTPR entities impacted by this rule.

Reporting Cybersecurity Incidents. The lack of reporting of significant cybersecurity incidents impedes TSA's ability to analyze potential cybersecurity risk information and recognize trends that warrant a Federal and industry response to address emerging threats.

Cybersecurity Training Program. Without the collection of cybersecurity training programs from owner/operators subject to the regulatory requirements, TSA would be unable to verify if regulated owner/operators are fulfilling the requirements of this proposed regulation or provide feedback when a security training program warrants modification. If TSA determines the program submitted meets the proposed regulatory requirements, the owner/operators would not need to submit additional programs to TSA unless or until amendments or updates are required. If modifications are required, the owner/operators would need to re-submit their training program as many times as necessary to obtain TSA approval. As such, it is not practical for TSA to reduce the frequency of collection. Having trained employees will reduce the number of successful cybersecurity incidents and the resulting need to respond to them, thereby increasing the ability of surface transportation networks to operate as expected.

Cybersecurity Training Records. Without a cybersecurity training records requirement, TSA would be unable to verify that a person subject to the CRM NPRM's regulatory requirements is complying with those requirements in the manner and schedule stipulated in their TSA-approved cybersecurity training program. A less frequent retention schedule would adversely affect the inspection process and impede determination of compliance with a regulatory requirement.

Cybersecurity Assessment Plan (CAP). Without a means of collecting this information, TSA would be unable to confidently ensure that entities have sufficient plans to assess the effectiveness of their programs as necessary to identify, prevent, detect, and respond to cybersecurity threats.

Physical Security Coordinator. TSA is responsible for sharing intelligence and other risk information relevant to the transportation industry. Lack of physical security coordinator information impedes TSA's ability to share information, potentially resulting in diminished capability for industry and the government to assess and respond to threats, incidents, and other security-related actions.

Reporting Significant Physical Security Concerns. The lack of reporting of significant physical security concerns impedes TSA's ability to analyze potential security-risk information and recognize trends that warrant a Federal and industry response to address identified threats.

Without this information collection, DHS would be hindered in its ability to quickly obtain information needed to address imminent, serious, quickly moving, and rapidly-evolving threats to these systems, which is key to national and economic security. TSA would be impeded without this foundational posture information for the covered owner/operators. Reducing the vulnerability of "Higher-Risk" pipelines, railroads, rail transit systems, and

OTRB operations and infrastructure to cybersecurity threats is fundamental to securing our Nation's traveling public and economic security.

7. Explain any special circumstances that require the collection to be conducted in a manner inconsistent with the general information collection guidelines in 5 CFR 1320.5(d)(2).

Under 5 CFR 1320.5(d)(2)(i), agencies must obtain OMB approval to respondents to report information to the agency more often than quarterly. Quarterly reporting of cybersecurity incidents would not meet the security needs that are the basis for this information collection. Under the proposed rule, and TSA's SDs, cybersecurity incidents must be reported within 24 hours. This timing is critical to ensure the government has the information it needs to protect national and economic security in the event of a cyber-attack.

Owner/operators are required to maintain training records for 5 years and surface security records for 7 years so that TSA may inspect for compliance. A less frequent retention schedule would adversely affect the inspection process and impede determination of compliance with a regulatory requirement.

While the rule does not specify that other information be reported more frequently than quarterly, it does require information to be current. For example, owner/operators are required to notify TSA within seven days of changes to information regarding cybersecurity coordinators. *See* proposed 49 CFR 1580.311, 1582.211, and 1586.211. If an owner/operator makes frequent changes to these designated points of contact, they may have to provide information more frequently than quarterly. Similarly, the proposed rule requires notifications to TSA within 15 days of any change to the Cybersecurity Incident Response Plan. *See* proposed 49 CFR 1580.327, 1582.227, and 1586.227. TSA is not mandating updates more frequently than quarterly unless the owner/operator is making frequent changes. TSA does not, however, anticipate that these or similar reporting would likely occur with less than quarterly frequency.

Otherwise, no special circumstances exist that would require the collection to be conducted in a manner inconsistent with the general information collection guidelines in 5 CFR 1320.5(d)(2).

8. Describe efforts to consult persons outside the agency to obtain their views on the availability of data, frequency of collection, the clarity of instructions and recordkeeping, disclosure, or reporting format (if any), and on the data elements to be recorded, disclosed, or reported. If applicable, provide a copy and identify the date and page number of publication in the Federal Register of the agency's notice, required by 5 CFR 1320.8(d) soliciting comments on the information collection prior to submission to OMB. Summarize public comments received in response to that notice and describe actions taken by the agency in response to these comments. Specifically address comments received on cost and hour burden.

On November 30, 2022, TSA published an Advanced Notice of Proposed Rulemaking (ANPRM) in docket TSA–2022–0001.[22] The purpose of the ANPRM was to inform of an upcoming rulemaking that would enhance cyber risk management policies for surface transportation modes regulated by TSA.

DHS received a total of 39 submissions at the close of the comment period on February 1, 2023; 36 public comment submissions via www.regulations.gov and three comment submissions, considered to contain SSI, were delivered directly to TSA. While TSA did receive comments related to the overall costs related to implementation and compliance with the proposed rule, the comments did not specifically address Information Collection related costs.

On November 7, 2024, TSA published the CRM NPRM, which will provide a 60-day public comment period. [23]

9. Explain any decision to provide any payment or gift to respondents, other than remuneration of contractors or grantees.

No payment or gift will be provided to respondents.

10. Describe any assurance of confidentiality provided to respondents and the basis for the assurance in statute, regulation, or agency policy.

While there is no assurance of confidentiality provided to respondents, TSA protects information collected from disclosure to the extent appropriate under applicable provisions of the Freedom of Information Act, Federal Information Security Management Act, E-Government Act, and Privacy Act of 1974. TSA would also appropriately treat any information collected that it determines is SSI and/or Personally Identifiable Information (PII), consistent with the requirements of 49 CFR part 1520 and OMB Guidance, M-07-16.

Also, to the extent permissible under the law, DHS will seek to protect the trade secrets and commercial and financial information of the pipeline owner/operators. *See* 49 CFR part 1520. In addition, any PII associated with reported incidents is handled in accordance with the System of Records Notices for DHS/TSA-001 Transportation Security Enforcement Record System 79 FR 6609 (February 4, 2014); and DHS/TSA-011 Transportation Security Intelligence Service Files, 75 FR 18867 (April 13, 2010).

For defensive measures and indicators shared under CISA's framework, Federal entities are required to apply appropriate controls to protect the confidentiality of cyber threat indicators that contain personal information of a specific individual or information that identifies a specific individual that is directly related to a cybersecurity threat or a use authorized under CISA to the greatest extent practicable. 6 U.S.C. 1504(b).

[22] 87 FR 73257 (Nov. 30, 2022).
[23] 89 FR 88488 (Nov. 7, 2024).

Additionally, to the extent that owner/operators provide TSA or CISA information that contains SSI, such information is not publicly releasable if doing so would be detrimental to transportation security. 49 CFR 1520.15(a).

11. Provide additional justification for any questions of sensitive nature, such as sexual behavior and attitudes, religious beliefs, and other matters that are commonly considered private.

No questions of a sensitive nature will be posed during the information collection.

12. Provide estimates of hour and cost burden of the collection of information.

In the first year, TSA estimates this collection applies to 73 freight railroad owner/operators, 34 PTPR owner/operators, 71 OTRB owner/operators, and 115 pipeline owner/operators, for a total of 293 respondents. TSA expects slight growth in freight railroad, PTPR, and OTRB modes during the next 3 years, with the number of pipeline owner/operators anticipated to remain the same. The number of respondents for each mode is depicted in Table 2.

Table 2: Number of Respondents

Mode	Year 1	Year 2	Year 3	3-Year Total	Average Annual Respondents
Freight Rail	73	74	74	221	74
PTPR	34	35	36	105	35
OTRB	71	72	74	217	72
Pipelines	115	115	115	345	115
Total	**293**	**296**	**299**	**888**	**296**

To determine opportunity costs, TSA uses data from the Bureau of Labor Statistics (BLS) to determine unloaded wage[24] rates for occupations involved in the information collection, by mode. Footnotes with links to the information are provided. Next, TSA used compensation data from BLS to calculate a compensation factor,[25] then multiplied the unloaded wage rates by the compensation factor to derive fully-loaded wage rates. The wage rates are depicted in Tables 3A-3C.

Table 3A: Freight Rail Wage Rates

	Unloaded Wage Rate	Compensation Factor	Fully-loaded Wage Rate
	A	B	C = A x B
Corporate Security Manager	$58.06[26]	1.480	$85.93
Cybersecurity Coordinator	$85.88[27]		$127.10
Cybersecurity Operations Manager	$85.88		$127.10
Cybersecurity Analyst	$45.50[28]		$67.34

[24] Unloaded wages are straight wages only and do not include benefits such as health insurance, retirement contributions, and other fringe benefits.
[25] The compensation factor accounts for compensation in addition to wages.
[26] BLS. May 2022 National Industry-Specific Occupational Employment and Wage Estimates. NAICS 482000 - Rail Transportation. OCC 11-1021 General and Operations Managers. https://www.bls.gov/oes/current/naics3_482000.htm. Accessed May 1, 2023.
[27] BLS. May 2022 National Industry-Specific Occupational Employment and Wage Estimates. NAICS 482000 - Rail Transportation. OCC 11-3021 Computer and Information Systems Managers. https://www.bls.gov/oes/2022/May/naics3_482000.htm. Accessed May 1, 2023.

Network/Systems Administrator	$43.67[29]		$64.63
Audit Manager	$62.60[30]		$92.65
Administrative Assistant	$27.31[31]		$40.42
Attorney	$87.98[32]		$130.21

Note: Calculations may not be exact due to rounding.

Table 3B: PTPR/OTRB Wage Rates

	Unloaded Wage Rate	Compensation Factor	Fully-loaded Wage Rate
	A	B	C = A x B
Corporate Security Manager	$41.92[33]	1.480	$62.04
Cybersecurity Coordinator	$71.50[34]		$105.82
Cybersecurity Operations Manager	$71.50		$105.82
Cybersecurity Analyst	$42.67[35]		$63.15
Network/Systems Administrator	$42.99[36]		$63.63
Audit Manager	$40.84[37]		$60.44
Administrative Assistant	$20.32[38]		$30.07
Attorney	$49.11[39]		$72.68

[28] BLS. May 2022 National Industry-Specific Occupational Employment and Wage Estimates. NAICS 482000 - Rail Transportation. OCC 15-1240 Database and Network Administrators. https://www.bls.gov/oes/2022/May/naics3_482000.htm. Accessed May 1, 2023.

[29] BLS. May 2022 National Industry-Specific Occupational Employment and Wage Estimates. NAICS 482000 - Rail Transportation. OCC 15-1244 Network and Computer Systems Administrators. https://www.bls.gov/oes/2022/May/naics3_482000.htm. Accessed May 1, 2023.

[30] BLS. May 2022 National Industry-Specific Occupational Employment and Wage Estimates. NAICS 482000 - Rail Transportation. OCC 11-3012 Administrative Services Managers. https://www.bls.gov/oes/2022/May/naics3_482000.htm. Accessed May 1, 2023.

[31] BLS. May 2022 National Industry-Specific Occupational Employment and Wage Estimates. NAICS 482000 - Rail Transportation. OCC 43-6010 Secretaries and Administrative Assistants. https://www.bls.gov/oes/2022/May/naics3_482000.htm. Accessed May 1, 2023.

[32] BLS. May 2022 National Industry-Specific Occupational Employment and Wage Estimates. NAICS 482000 - Rail Transportation. OCC 23-1011 Lawyer. https://www.bls.gov/oes/2022/May/naics3_482000.htm. Accessed May 1, 2023.

[33] BLS. May 2022 National Industry-Specific Occupational Employment and Wage Estimates. NAICS 485000 - Transit and Ground Passenger Transportation. OCC 11-1021 General and Operations Managers. . Accessed May 1, 2023.

[34] BLS. May 2022 National Industry-Specific Occupational Employment and Wage Estimates. NAICS 485000 - Transit and Ground Passenger Transportation. OCC 11-3021 Computer and Information Systems Managers. . Accessed May 1, 2023.

[35] BLS. May 2022 National Industry-Specific Occupational Employment and Wage Estimates. NAICS 485000 - Transit and Ground Passenger Transportation. OCC 15-1240 Database and Network Administrators and Architects. . Accessed May 1, 2023.

[36] BLS. May 2022 National Industry-Specific Occupational Employment and Wage Estimates. NAICS 485000 - Transit and Ground Passenger Transportation. OCC 15-1244 Network and Computer Systems Administrators. . Accessed May 1, 2023.

[37] BLS. May 2022 National Industry-Specific Occupational Employment and Wage Estimates. NAICS 485000 - Transit and Ground Passenger Transportation. OCC 11-3012 Administrative Services Managers. . Accessed May 1, 2023.

[38] BLS. May 2022 National Industry-Specific Occupational Employment and Wage Estimates. NAICS 485000 - Transit and Ground Passenger Transportation. OCC 43-6010 Secretaries and Administrative Assistants. . Accessed May 1, 2023.

[39] BLS. May 2022 National Industry-Specific Occupational Employment and Wage Estimates. NAICS 485000 - Transit and Ground Passenger Transportation. OCC 23-1011 Lawyer.

Note: Calculations may not be exact due to rounding.

Table 3C: Pipelines Wage Rates

	Unloaded Wage Rate	Compensation Factor	Fully-loaded Wage Rate
	A	B	C = A x B
Corporate Security Manager	$86.76[40]	1.480	$126.92
Cybersecurity Coordinator	$79.79[41]		$118.08
Cybersecurity Operations Manager	$79.79		$118.08
Cybersecurity Analyst	$47.97[42]		$70.99
Network/Systems Administrator	$41.36[43]		$61.21
Audit Manager	$93.31[44]		$138.10
Administrative Assistant	$27.45[45]		$40.63
Attorney	$189.33[46]		$280.21

TSA uses the fully-loaded wages rates in Tables 3A-3C, then depending on the individuals and the amount of time performing each information collection activity, blends them into fully-loaded wage rates for each. To calculate the hour burden costs, TSA multiplies the number of hours to perform an information collection activity by the applied wage rate. TSA estimates the total hour burden over the next 3 years to be 318,083 hours (average 106,028 hours per year). The total hour burden cost is estimated to be $27,915,239 (average of $9,305,080 per year). These calculations are depicted in Table 4.

https://www.bls.gov/oes/2022/May/naics3_485000.htm. Accessed May 1, 2023.

[40] BLS. May 2022 National Industry-Specific Occupational Employment and Wage Estimates. NAICS 486000 – Pipeline Transportation. OCC 11-1021 General and Operations Managers. . Accessed July 17, 2023.

[41] BLS. May 2022 National Industry-Specific Occupational Employment and Wage Estimates. NAICS 486000 – Pipeline Transportation. OCC 11-3021 Computer and Information Systems Managers. https://www.bls.gov/oes/2022/May/naics3_486000.htm. Accessed July 17, 2023.

[42] BLS. May 2022 National Industry-Specific Occupational Employment and Wage Estimates. NAICS 486000 – Pipeline Transportation. OCC 15-1212 Computer Systems Analysts. . Accessed July 17, 2023.

[43] BLS. May 2022 National Industry-Specific Occupational Employment and Wage Estimates. NAICS 486000 – Pipeline Transportation. OCC 15-1244 Network and Computer Systems Administrator. . Accessed July 17, 2023.

[44] BLS. May 2022 National Industry-Specific Occupational Employment and Wage Estimates. NAICS 486000 – Pipeline Transportation. OCC 11-3012 Administrative Services Managers. Accessed July 17, 2023.

[45] BLS. May 2022 National Industry-Specific Occupational Employment and Wage Estimates. NAICS 486000 – Pipeline Transportation. OCC 43-6010 Secretaries and Administrative Assistants. . Accessed July 17, 2023.

[46] BLS. May 2022 National Industry-Specific Occupational Employment and Wage Estimates. NAICS 486000 – Pipeline Transportation. OCC 23-1011 Lawyers. . Accessed July 17, 2023.

		Table 4: Compliance Documentation Requirements: Submission Reporting and Recordkeeping Hour Burden and Hour Burden Costs												
Mode	Time Per Response (hrs)	Number of Responses			Hour Burden			Total 3yr Hour Burden	Average Annual Responses	Average Annual Hour burden	Applied Wage Rate	Hour Burden Cost			Total Hour Burden Cost
		Yr 1	Yr 2	Yr 3	Yr 1	Yr 2	Yr 3					Yr 1	Yr 2	Yr 3	
Calculation	A	B	C	D	E = A X B	F = A x C	G = A x D	H = E + F +G	I = (B+C+D)/3	J=A/3	K	L = E xK	M= F x K	N = G xK	O = L+M+N
		Cybersecurity Evaluation (CSE) - Owner/operator holds for TSA inspection (Record keeping)													
Freight Rail[47]	40	73	74	74	2,920	2,945	2,970	8,835	74	2,947	$66.88	$195,284	$196,944	$198,618	$590,847
PTPR	40	34	35	37	1,360	1,400	1,480	4,240	35	1,400	$63.47	$86,325	$88,864	$93,942	$269,131
Pipelines[48]	120	115	115	115	13,800	13,800	13,800	41,400	115	13,800	$68.77	$949,044	$949,044	$949,044	$2,847,133
		Cybersecurity Operational Implementation Plan (COIP) Submission - Submitted to TSA for review and approval (Reporting)													
Freight Rail	4	73	1	1	292	2	3	297	25	100	$129.07	$37,689	$320	$323	$38,332
PTPR	4	34	1	2	136	4	8	148	12	48	$89.54	$12,177	$358	$716	$13,252
Pipelines	4	115	0	0	460	0	0	460	38	152	$199.79	$91,904	$0	$0	$91,904
		Accountable Executive Information Submission - Included in COIP (Reporting)													
Freight Rail	3	121	122	123	363	366	369	1,098	122	366	$130.11	$47,229	$47,631	$48,036	$142,896
PTPR	3	68	70	74	204	210	222	636	71	212	$78.46	$16,005	$16,476	$17,418	$49,899
Pipelines	3	205	205	205	615	615	615	1,845	205	615	$254.01	$156,214	$156,214	$156,214	$468,642
		Cybersecurity Coordinator Information Submission - Included in COIP (Reporting)													
Freight Rail	3	194	27	27	582	80	80	742	83	249	$129.59	$75,421	$10,319	$10,385	$96,125
PTPR	3	102	15	15	306	45	45	396	44	132	$84.00	$25,704	$3,780	$3,780	$33,264
Pipelines	6	319	42	42	1,916	255	255	2425	134	804	$226.90	$434,679	$57,832	$57,832	$550,343
		Initial Identification of Critical Cyber Systems and Network Architecture - Included in COIP (Record keeping)													
Freight Rail	244	73	1	1	17,841	152	153	18,146	25	6,100	$97.59	$1,741,201	$14,800	$14,926	$1,770,927
PTPR	244	34	1	2	8,310	244	489	9,043	12	2,928	$85.14	$707,486	$20,808	$41,617	$769,912
Pipelines	244	115	0	0	28,106	-	-	28,106	38	9,272	$93.82	$2,636,788	$0	$0	$2,636,788
		Annual Identification of Critical Cyber Systems[49] - Included in COIP (Recordkeeping)													
Freight Rail	121	0	73	74	0	8,818	8,893	17,712	49	5,929	$83.87	$0	$739,640	$745,926	$1,485,566
PTPR	121	0	34	35	0	4,107	4,228	8,335	23	2,783	$62.40	$0	$256,277	$263,814	$520,091
Pipelines	121	0	115	115	0	13,892	13,892	27,784	77	9,317	$81.02	$0	$1,125,591	$1,125,591	$2,251,182
		Description of how detection and monitoring security outcomes are met - Included in COIP (Record keeping)													
Freight Rail	N/A	73	1	1	N/A	N/A	N/A	N/A			$129.07	N/A	N/A	N/A	N/A
PTPR	N/A	34	1	2	N/A	N/A	N/A	N/A			$89.54	N/A	N/A	N/A	N/A

[47] Freight Rail and PTPR Time Per Response values from ICR 1652-0074.

[48] Pipelines Time Per Response value from SME estimate.

[49] Column I is a blended wage rate attributing 30 hours to the cybersecurity coordinator, 24.8 to network/system administrator, and 66 hours to the Cybersecurity Analyst.

Pipelines	N/A	115	0	0	N/A	N/A	N/A	N/A			$199.79	N/A	N/A	N/A	N/A
		Description of how protective security outcomes are met - Included in COIP (Record keeping)													
Freight Rail	N/A	73	1	1	N/A	N/A	N/A	N/A			$129.07	N/A	N/A	N/A	N/A
PTPR	N/A	34	1	2	N/A	N/A	N/A	N/A			$89.54	N/A	N/A	N/A	N/A
Pipelines	N/A	115	0	0	N/A	N/A	N/A	N/A			$199.79	N/A	N/A	N/A	N/A
		Initial Cybersecurity Training Plan Development and Submission - Included in COIP (Reporting)													
Freight Rail	68	73	1	1	4,941	42	42	5,026	25	1,700	$86.21	$425,962	$3,621	$3,651	$433,234
PTPR	68	34	1	2	2,301	68	135	2,504	12	816	$62.24	$143,242	$4,213	$8,426	$155,881
Pipelines	68	115	0	0	7,784	0	0	7,784	38	2,584	$128.82	$1,002,740	$0	$0	$1,002,740
		Modified Cybersecurity Training Plan Development and Submission - Included in COIP (Reporting)													
Freight Rail	18.75	66	0	0	1,232	0	0	1,232	33	619	$86.21	$106,195	$0	$0	$106,195
PTPR	18.75	31	0	0	574	0	0	574	10	188	$62.24	$35,711	$0	$0	$35,711
Pipelines	18.75	104	0	0	1,941	0	0	1,941	35	656	$128.82	$249,990	$0	$0	$249,990
		Cybersecurity Training Recordkeeping - Included in COIP (Record keeping)													
Freight Rail	0.017	134,504	135,064	135,626	2,242	2,251	2,260	6,753	135,065	2,701	$40.55	$90,901	$91,279	$91,659	$273,839
PTPR	0.017	344,632	348,472	352,355	5,744	5,808	5,873+	17,424	348,486	6,970	$30.17	$173,297	$175,228	$177,180	$525,705
Pipelines	0.017	45,908	46,194	46,482	765	770	775	2,310	46,195	924	$40.76	$31,185	$31,379	$31,575	$94,138
		Cybersecurity Incident Response Plan (CIRP) - Included in COIP (Record keeping)													
Freight Rail	80	73	1	0	5,840	40	0	5,920	25	2,000	$127.51	$744,676	$5,101	$0	$749,776
PTPR	80	34	1	2	2,720	40	80	2,960	12	960	$106.16	$288,760	$4,246	$8,493	$301,500
Pipelines	80	115	0	0	9,200	0	0	9,200	38	3,040	$118.47	$1,089,930	$0	$0	$1,089,930
		CIRP Annual Exercise - Included in COIP (Record keeping)													
Freight Rail	40	73	74	74	2,920	2,960	2,960	8,840	74	2,960	$127.51	$372,338	$377,438	$377,438	$1,127,215
PTPR	40	34	35	37	1,360	1,400	1,480	4,240	35	1,400	$127.51	$173,418	$178,518	$188,719	$540,655
Pipelines	40	115	115	115	4,600	4,600	4,600	13,800	115	4,600	$118.47	$544,965	$544,965	$544,965	$1,634,895
		Cybersecurity Assessment Plan (CAP) for TSA Approval (Reporting)													
Freight Rail	14	73	74	74	1,022	2,960	2,960	3,094	74	1,036	$75.73	$77,401	$224,174	$224,174	$525,748
PTPR	14	34	35	37	476	1,400	1,480	1,484	35	490	$69.54	$33,100	$97,354	$102,917	$233,372
Pipelines	14	115	115	115	1,610	4,600	4,600	4,830	115	1,610	$76.57	$123,281	$352,232	$352,232	$827,746
		CAP Annual Report of Scheduled Testing of COIP - 30 % annually and 100% every 3 years – A part of CAP (Reporting)													
Freight Rail	30	73	74	74	2,190	2,207	2,224	6,621	74	2,220	$65.93	$144,381	$145,507	$146,643	$436,531
PTPR	30	34	35	37	1,020	1,059	1,100	3,179	35	1,050	$63.64	$64,913	$67,400	$69,981	$202,294
Pipelines	30	115	115	115	3,450	3,450	3,450	10,350	115	3,450	$65.34	$225,410	$225,410	$225,410	$676,231
		Compliance Recordkeeping													
Freight Rail	2	73	74	74	146	2,960	2,960	442	74	148	$40.55	$5,920	$120,026	$120,026	$245,972
PTPR	2	34	35	37	68	1,400	1,480	212	35	70	$30.17	$2,052	$42,239	$44,653	$88,943
Pipelines	2	115	115	115	230	4,600	4,600	690	115	230	$40.76	$9,374	$187,483	$187,483	$384,341
		Physical Security Coordinator Information Submission (Reporting)													
Pipelines	0.5	261	34	34	131	17	17	165	110	55	$128.82	$16,814	$2,190	$2,190	$21,194

		Report Significant Physical Security Concerns to TSA (Reporting)													
Pipelines	0.05	2,908	2,908	2,908	145	145	145	436	2,908	145	$128.82	$18,730	$18,730	$18,730	$56,191,560
Total Annual Responses									**535,070**						
Total Hour Burdens and Costs					**158,278**	**79,780**	**80,025**	**318,083**		**99,790**		**$15,123,729**	**$6,393,002**	**$6,398,508**	**$27,915,239**

Note: Calculations may not be exact due to rounding.

13. Provide an estimate of annualized capital and start-up costs. (Do not include the cost of any hour burden shown in Items 12 and 14).

TSA does not estimate a cost to industry beyond the burden detailed in the previous section.

14. Provide estimates of annualized cost to the Federal Government. Also, provide a description of the method used to estimate cost, and other expenses that would not have been incurred without this collection of information.

TSA estimates there are 12 information collection activities that will be processed and reviewed by TSA personnel. As previously noted, the government burden for cybersecurity incident reports is reported in OMB control number 1670-0037. TSA uses the Modular Cost model[50] to determine the applicable wage rates for personnel processing and reviewing data for this information collection. The pay band and wage rate information is presented in Table 5.

Table 5: Applicable Pay Bands and Wage Rates

Pay Band	Wage Rate
H Band	$56.80
I Band	$77.75
J Band	$91.56
K Band	$107.38

The total government cost for this information collection is expected to be $4,899,949 over 3 years, or an average annual cost of $1,633,316. The government burden and cost are displayed in Table 6.

Table 6: Government Burden and Cost

Activity	Time Per Response (hrs.)	Number of Responses			Hour Burden			Total Hour Burden	Applied Wage Rate	Hour Burden Cost			Total Hour Burden Cost
		Year 1	Year 2	Year 3	Year 1	Year 2	Year 3			Year 1	Year 2	Year 3	
	A	B	C	D	E = A x B	F = A x C	G = A x D	H = E + F +G	I	J = E x I	K = F x I	L = G x I	M = J + K + L
Cybersecurity Evaluation (CSE) Processing [51]	4.0	222	224	226	888.0	896.0	904.0	2,688.0	$84.66	$75,173.64	$75,850.88	$76,528.12	$227,552.64
COIP Review and Approval[52]	50.0	222	2	3	11,100.0	78.5	128.7	11,307.2	$94.09	$1,044,412.32	$7,383.81	$12,111.14	$1,063,907.27
COIP Legal Review[53]	4.0	111	1	1	444.0	2.6	2.7	449.3	$107.38	$47,676.72	$279.66	$290.37	$48,246.75

[50] TSA, Office of Finance and Administration, FY2022 Modular Cost Data.
[51] TSA uses a blended wage rate of 50% H band and 50% I band employees.
[52] Blended wage rate calculated by assuming three TSA employees spend 14 hours on review are at a J-Band Level, and two regional employees spend additional 4 hours are at a K-Band Level.
[53] TSA estimates 50 percent of submitted COIPs will require a legal review.

Accountable Executive Information Processing[54]	5.0	394	45	48	1,971.8	224.7	239.8	2,436.2	$84.66	$166,919.77	$19,023.65	$20,296.87	$206,240.28
Cybersecurity Coordinator Information Processing[55]	5.0	616	70	73	3,081.8	347.8	362.9	3,792.5	$84.66	$260,886.82	$29,446.50	$30,721.77	$321,055.08
Initial Cybersecurity Training Plan Processing[56]	40.0	222	2	3	8,880.0	62.8	103.0	9,045.8	$84.66	$751,736.40	$5,314.64	$8,717.23	$765,768.27
Resubmitted Cybersecurity Training Plans[57]	4.0	200	0	0	799.2	-	-	799.2	$84.66	$67,656.28	$0.00	$0.00	$67,656.28
Cybersecurity Training Records Inspections[58]	4.0	222	224	226	888.0	894.3	904.6	2,686.9	$56.80	$50,438.40	$50,794.99	$51,379.88	$152,613.27
Cybersecurity Incident Response Plan (CIRP) Processing[59]	4.0	222	1	1	888.0	5.0	5.2	898.2	$84.66	$75,173.64	$424.69	$440.95	$76,039.28
Cybersecurity Assessment Plan (CAP) Processing[60]	32.0	222	224	226	7,104.0	7,165.5	7,228.8	21,498.3	$84.66	$601,389.12	$606,597.64	$611,955.55	$1,819,942.31
Physical Security Coordinator Information Processing[61]	0.17	261	36	36	43.6	6.0	6.0	55.6	$56.80	$2,476.22	$341.48	$341.48	$3,159.18
Significant Physical Security Concerns Reports Processing[62]	0.07	8,723	8,723	8,723	581.8	581.8	581.8	1,745.5	$84.66	$49,256.15	$49,256.15	$49,256.15	$147,768.46
Total Hour Burdens and Costs					**36,670.2**	**10,265.1**	**10,467.5**	**57,402.8**		**$3,193,195.47**	**$844,714.08**	**$862,039.52**	**$4,899,949.07**

15. Explain the reasons for any program changes or adjustments reported in Items 13 or 14 of the OMB Form 83-I.

This is both a new collection that incorporates requirements currently covered by existing OMB numbers for the previously issued SDs plus new requirements proposed in the NPRM. Upon approval of the new ICR and publication of a final rule, TSA will amend, or as appropriate rescind, the current ICRs associated with TSA SDs or other regulatory requirements currently in effect.

[54] TSA uses a blended wage rate of 50% H band and 50% I band employees.
[55] TSA uses a blended wage rate of 50% H band and 50% I band employees.
[56] TSA uses a blended wage rate of 50% H band and 50% I band employees.
[57] TSA uses a blended wage rate of 50% H band and 50% I band employees.
[58] TSA assumes this task will be done by an H band employee.
[59] TSA uses a blended wage rate of 50% H band and 50% I band employees.
[60] TSA uses a blended wage rate of 50% H band and 50% I band employees.
[61] TSA assumes this task will be done by an H band employee.
[62] TSA uses a blended wage rate of 50% H band and 50% I band employees.

16. For collections of information whose results will be published, outline plans for tabulation and publication. Address any complex analytical techniques that will be used. Provide the time schedule for the entire project, including beginning and ending dates of the collection of information, completion of report, publication dates, and other actions.

The information collection will not be published.

17. If seeking approval to not display the expiration date for OMB approval of the information collection, explain the reasons that display would be inappropriate.

Not applicable.

18. Explain each exception to the certification statement identified in Item 19, "Certification for Paperwork Reduction Act Submissions," of OMB Form 83-I.

No exceptions noted.