*INFORMATION COLLECTION SUPPORTING STATEMENT*

# Cybersecurity Measures for Surface Modes
# OMB control number 1652-0074
# EXP. 04/30/2023

***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).***

Congress granted the TSA Administrator authority for the security of the transportation system.[1] Under the specific authorities of 49 U.S.C. § 114, TSA may take immediate action to impose measures to protect transportation security without providing notice or an opportunity for comment.[2] The cybersecurity threats to surface transportation infrastructure that necessitate these collections are consistent with TSA's mission, as well as TSA's 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." *See* 49 U.S.C. § 114(d).

Additionally, under 49 U.S.C. § 114(*l*)(2),[3] TSA has the authority to issue security directives if the Administrator of TSA determines that a regulation or security directive must be issued immediately in order to protect transportation security. TSA also has authority, at the discretion of the Administrator, to assist another Federal agency in carrying out its authority in order to address a threat to transportation. *See* 49 U.S.C. § 114(m).[4]

The United States (U.S.) surface transportation system is a complex interconnected and largely open network including freight railroads, public transportation and passenger rail systems, and over-the-bus (OTRB) service. Many of these surface transportation modes employ increasingly integrated cyber and physical systems that operate daily in close coordination with and proximity to each other nationwide. These cyber systems are under constant and escalating risk due to cyber attacks.

---

[1] *See* section 114(d) of title 49, United States Code (U.S.C.). Under 49 U.S.C. § 114(f)(3) and (4), TSA may "develop policies, strategies, and plans for dealing with the threats ... including coordinating countermeasures with appropriate departments, agencies, and instrumentalities of the United States."

[2] TSA issues security directives for surface transportation operators under the statutory authority of 49 U.S.C. § 114(l)(2)(A). This provision, from section 101 of the Aviation and Transportation Security Act, Pub. L. 107-71 (115 Stat. 597; Nov. 19, 2001), states: "Notwithstanding any other provision of law or executive order (including an executive order requiring a cost-benefit analysis), if the Administrator 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."

[3] Notwithstanding any other provision of law or executive order (including an executive order requiring a cost-benefit analysis), if the Administrator 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.

[4] 49 U.S.C. § 114(m) grants the TSA Administrator the same authority as the Administrator of the Federal Aviation Administration under 49 U.S.C. § 106(m), and is applicable to all modes of transportation.

On November 30, 2021, OMB approved TSA's request for an emergency approval of an information collection to address the ongoing cybersecurity threat to surface transportation and associated infrastructure. On December 17, 2021,[5] TSA issued the Security Directive (SD) 1580-21-01 and SD 1582-21-02 series,[6] which became effective on December 31, 2021, mandating that TSA-specified Owner/Operators of higher-risk freight railroads and "higher-risk" passenger railroads and rail transit systems, respectively, implement an array of cybersecurity measures to prevent disruption and degradation to their infrastructure. The scope of these security directives align with the railroads and rail transit systems required to report significant security incidents to TSA under 49 CFR 1570.203. On that same date, TSA also issued an "Information Circular" (IC), which contains non-binding recommendations with the same measures for railroad Owner/Operators, public transportation agencies, rail transit system Owner/Operators, and certain OTRB Owner/Operators not specifically covered under the SD 1580-21-01 or SD 1582-21-02 series. The requirements in the security directives and the recommendations in the IC allow TSA to execute its security responsibilities within the surface transportation industry, through reporting of cybersecurity incidents; designating a cybersecurity coordinator; conducting a cybersecurity risk assessment; implementing a TSA-approved Cybersecurity Implementation Plan; maintaining an up-to-date Cybersecurity Incident Response Plan; submitting a Cybersecurity Vulnerability Assessment; and establishing a Cybersecurity Assessment Program.

On April 7, 2022, TSA submitted an extension request to OMB, which was approved on October 25, 2022. *See* ICR Reference Number 202203-1652-003. On October 26, 2022, OMB approved TSA's request for an additional emergency approval, revising this information collection. *See* ICR Reference Number: 202210-1652-001. The collection covers both mandatory reporting and voluntary reporting of information. The OMB approval allowed for the additional institution of mandatory reporting requirements and collection of information voluntarily submitted. *See* ICR Reference Number: 202111-1652-003. TSA is now seeking renewal of this information collection for the maximum three-year approval period.

The request for a revised collection was necessary as a result of actions TSA took to address the ongoing cybersecurity threats to the United States' national and economic security posed by this threat to surface transportation and associated infrastructure. On October 18, 2022, TSA issued SD 1580/1582-2022-01, *Rail Cybersecurity Mitigation Actions and Testing*, which is complementary to the requirements in the previous directives. This security directive applies to Owner/Operators of the "higher-risk" freight railroads identified in 49 CFR 1580.101 and additional TSA-designated freight and passenger railroads. This security directive became effective on October 24, 2022. The emergency request did not affect the previously-approved collection for SD 1580-21-01 and SD 1582-21-01, which remain in effect, mandating that TSA-specified Owner/Operators of higher-risk railroads and rail

[5] On November 30, 2021, OMB approved TSA's request for the new information collection to address the ongoing cybersecurity threat to surface transportation and associated infrastructure. On April 7, 2022, TSA submitted an extension request to OMB, which was approved on October 25, 2022. *See* ICR Reference Number 202203-1652-003.

[6] The numbering methodology for security directives uses regulatory provisions as a shorthand reference to the sector. For example, "1580" refers to freight rail owner/operators regulated under 49 CFR part 1580, "1582" refers passenger rail and public transportation agencies regulated under 49 CFR part 1582, and "1584" would refer to OTRB owner/operators regulated under 49 CFR part 1584.

transit systems, respectively, implement an array of cybersecurity measures to prevent disruption and degradation to their infrastructure.

In addition, the emergency request did not affect the previously-issued IC, which remains in effect. The IC contains non-binding recommendations with the same measures for Owner/Operators of railroads, public transportation systems, rail transit systems, and certain OTRB operations not specifically covered under SDs 1580-21-01 or 1582-21-01.

***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.***

The information collected pursuant to the requirements in the security directives and the recommendations in the IC allow TSA to execute its security responsibilities within the surface transportation industry, through awareness of potential security incidents and suspicious activities.

***A. SD 1580/82-2022-01 Series***

This security directive series issued in 2022, to complement those issued in 2021, includes the following information collection:

1. Submission of a Cybersecurity Implementation Plan to TSA for approval that addresses how the Owner/Operator will achieve each of the following prescribed objectives in the security directive:
    - Identification of the Owner/Operator's Critical Cyber Systems;
    - Implementation of network segmentation policies and controls to ensure that the Operational Technology system can continue to safely operate in the event that an Information Technology system has been compromised;
    - Implementation of access control measures to secure and prevent unauthorized access to critical cyber systems;
    - Implementation of continuous monitoring and detection policies and procedures to detect cybersecurity threats and correct anomalies that affect Critical Cyber System operations; and
    - Reduction of 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.

2. Submission of an Annual Audit Plan for the Cybersecurity Assessment Program 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.

3. Documentation provided to TSA upon request as necessary to establish compliance.

***B. SD 1580-21-01, SD 1582-21-01, and IC 2021-01 Series***

The security directives and the IC issued in 2021 remain in effect and include the following information collection requirements:

1. Provide contact information for a designated Cybersecurity Coordinator who is available to TSA 24/7 to coordinate cybersecurity practices and address any incidents that arise.

2. Report cybersecurity incidents to the Cybersecurity and Infrastructure Security Agency (CISA) within 24 hours of identification of a cybersecurity incident. 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. CISA has an approved information collection for cybersecurity incident reporting. *See* OMB control number 1670-0037.

3. Submit a cybersecurity incident response plan.

4. Complete a cybersecurity vulnerability assessment to address cybersecurity gaps using the form provided by TSA.

TSA, in conjunction with federal partners such as CISA, will use the reports of cybersecurity incidents to evaluate and respond to imminent and evolving cybersecurity incidents and threats as they occur, and as a basis for creating new cybersecurity policy moving forward. This monitoring will allow TSA and federal partners to take action to contain threats, take mitigating action, and issue timely warnings to similarly-situated entities against further spread of the threat. TSA and its federal partners will also use the information to inform timely modifications to cybersecurity requirements to improve transportation security and national economic security. TSA will use the collection of information to ensure compliance with TSA's cybersecurity measures required by the security directives and the recommendations under the IC.

The SD 1580-21-01, SD 1582-21-01, and IC 2021-01 took effect on December 31, 2021. As of this time, all Owner/Operators covered by the SDs are required to be in full compliance. The SD 1580/82-2022-01 series took effect on October 24, 2022. Within 90 days of the effective date of the security directives, Owner/Operators must submit their Cybersecurity Assessment Plan, and annually thereafter.

Owner/Operators can complete and submit the required information via email or other electronic options provided by TSA. Documentation of compliance for the Cybersecurity Assessment Program must be provided upon request. As the measures in the IC are voluntary, the IC does not require Owner/Operators to report on their compliance.

To the extent these requirements have not been already fulfilled, Owner/Operators can complete and submit the required information via email or other electronic options provided by TSA. Documentation of compliance must be provided upon request to TSA. As the measures in the IC are voluntary, the IC does not require Owner/Operators to report on their compliance.

Information submitted by the Owner/Operators to TSA as required by the security directive, and if voluntarily submitted under the IC, are deemed Sensitive Security Information (SSI) are protected in accordance with procedures meeting the transmission, handling, and storage requirements of SSI set forth in 49 CFR part 1520.[7]

[7] In addition, all data in TSA systems are statutorily required to comply with the Federal Information Security Modernization Act 2014 (FISMA) following the National Institute of Standards and Technology Special Publication 800.37 REV2 or Risk Management Framework, and other federal information security requirements including Federal Information Processing Standards 199 and Executive Order 14028. All systems, networks, servers, clouds and endpoints under the FISMA boundary are hardened to meet the Department of Defense (DOD) Security Technical Implementation Guidelines, as well as DHS Policy (4300.A) and TSA policy (TSA IA Handbook).

***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.***

***SD 1580/1582-22-01 Series Collection:***

TSA requires the following collection of information and maintenance of records to establish compliance with the SD 1580/1582-2022-01 Series:

- Cybersecurity Implementation Plan: Freight/Passenger Rail Owner/Operators must transmit their implementation plans to TSA electronically via a secure means. All implementation plans submitted by operators are considered SSI under the provisions of 49 CFR part 1520.

- Cybersecurity Assessment Program: Freight/Passenger Rail Owner/Operators must submit their cybersecurity assessment plans on an annual basis to TSA electronically via a secure means. All cybersecurity assessment plans submitted by operators are considered SSI under the provisions of 49 CFR part 1520.

- Records to Establish Compliance: Freight/Passenger Rail Owner/Operators must provide to TSA electronically, as part of a compliance inspection, documentation to establish their compliance with the security directive. Operator records provided to TSA to document compliance with the security directive are considered SSI under the provisions of 49 CFR part 1520.

***SD 1580-21-01, SD 1582-21-01, and IC 2021-01 Series Collection:***

In compliance with the Government Paperwork Elimination Act, the following fully electronic reporting options are available and continuing 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. CISA has an approved information collection for cybersecurity incident reporting. *See* OMB control number 1670-0037.

- For those Owner/Operators to whom the security directive applies, they can submit statements confirming that they have complied with requirements within the established deadlines or other electronic options provided by TSA. For convenience, TSA provides optional forms that can be submitted via email confirming completion (TSA SD-1580-21-01 Statement of Completion and TSA SD-1582-21-02 Statement of Completion) for each submission deadline.

- In addition, Owner/Operators are required by the security directive, and recommended under the IC, to develop a cybersecurity contingency/recovery plan to address cybersecurity gaps. Lastly, Owner/Operators are required by the security directive, and recommended under the IC, to conduct the assessment of their cybersecurity posture using *TSA Surface (Rail and Public Transportation) Cybersecurity Vulnerability Assessment* form, and submit the results to TSA. There are two methods for Owner/Operators to submit the information, which is considered SSI under 49 CFR part 1520 once completed. The first is via email and a password-protected document with the password being sent in a separate email. The second is to upload the document on a specific secure portal that TSA has established.

  Usability Study DHS CIO Requirement:
  TSA completed a Usability Study on the *TSA Surface (Rail and Public Transportation) Cybersecurity Vulnerability Assessment* form. All usability study participants were Surface Industry Stakeholders; two from Freight Rail and two from Public Transportation Passenger Rail systems. All of the participants were active users of the form. Participants found the instructions were easy to understand, and functionality was simple to use. Participants were confident about using the form as it was self-explanatory and easy to navigate. All participants completed the form without assistance and were familiar with the National Institute of Standards and Technology and questions were straight-forward. Further the participants found that the choice options of "yes" and "no" made the response selection clear. Participants provided comments for improvement, recommending an "n/a" choice option, and an additional column or supplemental document without the text character limitations in order to provide additional details to facilitate TSA inspection visit of compliance documentation. Also, participants recommended that questions be modal specific and/or tailored to the transportation sector. In addition, stakeholders provided feedback on the estimated time and level of effort burden. TSA examined the recommendations and will consider them for future action in the development of iterations of forthcoming information collection tools. TSA determined that the time burden estimate of 42 hours was a median of the validated time estimates the participants provided.

***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.***

***SD 1580/1582-22-01 Series Collection:***

TSA developed the requirements in consultation with CISA and in coordination with the Department of Transportation (DOT), Department of Defense (DOD), and other applicable agencies. TSA has determined that no other agency requires submission of the type of information TSA may collect related to its security directives.

***SD 1580-21-01, SD 1582-21-01, and IC 2021-01 Series Collection:***

The Department of Homeland Security (DHS) has a broad Memorandum of Understanding (MOU) with 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. There is no other similar information collection currently in place at DOT that specifically targets corporate-level cybersecurity planning and plan implementation in the surface modes of transportation.

Within DHS, TSA coordinates closely with CISA, which advances the Initiative's effort and secures the cybersecurity posture of the critical surface transportation sectors due to the interconnected systems and importance to the American way of life. TSA developed the requirements and recommendations, as applicable, in consultation with CISA and in coordination with DOT, DOD, and other agencies, as applicable. TSA requires reporting of certain information directly to CISA, which CISA shares with TSA to reduce duplication. Apart from the reporting to CISA under the security directive or IC, and provisions for sharing information with federal partners, TSA has determined that no other agency requires submission of the type of information collected via its security directives and IC from the same persons.

***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 does not have a significant impact on a substantial number of small businesses.

***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.***

Without these collections, DHS will be unable to address the critical, imminent threat of cyberattacks, such as ransomware, to the nation's surface transportation systems. Further, 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 and would be impeded if TSA did not have this foundational posture information for the covered Owner/Operators now in the light of this continuous threat. Reducing the vulnerability of higher-risk railroads, rail transit systems, and OTRB[8] operations and infrastructure to cybersecurity threats is fundamental to securing our nation's travelling public and economic security.

In addition, TSA will be unable to address the critical threat to the nation's freight railroad and passenger rail systems, which is reasonably likely to result in public harm. For example, if an attack occurred against a railway system and TSA did not have this collection, freight/passenger rail Owner/Operators may not have adequate cybersecurity measures or a Cybersecurity Implementation Plan and Cybersecurity Audit Program in place. These measures decrease the impact of a cybersecurity incident affecting critical infrastructure and increase an operator's awareness of possible vulnerabilities.

[8] The IC recommendation applies to OTRB Owner/Operators.

***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).***

This collection is conducted consistent with the information collection guidelines, except for those in 5 CFR 1320.5(d)(2)(i). This collection requires respondents to report information to the agency more often than quarterly. Quarterly reporting would not meet the security needs that is the basis for this information collection.

***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.***

TSA published a *Federal Register* notice, with a 60-day comment period soliciting comments of the collection of information. *See* 87 FR 68185 (November 14, 2022). Additionally, TSA published a 30-day notice in the *Federal Register*. *See* 87 FR 14628 (March 9, 2023). These notices did not generate any comments on the collection of information.

Please see the response to question #4 for the efforts that TSA made to consult externally with industry as well as federal partners.

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

No payment or gift is 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 reporting entities, 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, 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 Freight/Passenger Rail Owner/Operators. *See* 49 CFR part 1520. This collection is covered under the Privacy Impact Assessment (PIA), DHS/ALL/PIA-006 DHS General Contact Lists (June 15, 2007).

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).

***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 personal questions of a sensitive nature are posed during the information collection.

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

***SD 1580/1582-2022-01 Series Collection:***

The information collection required by SD 1580/1582-2022-01 Series would only apply to a total of 73 Owner/Operators to include the 38 higher-risk freight railroads identified in 49 CFR 1580.101, 30 railroads newly-designated by TSA based on risk, [9] and five of the passenger rail Owner/Operators operations identified in 49 CFR 1582.101 based on hosting one of the higher-risk freight rail operations.

**Cybersecurity Implementation Plan:** TSA estimates 73 entities will develop a Cybersecurity Implementation Plan, and the plan will be developed by a team consisting of a cybersecurity manager and four cybersecurity analysts/specialists. TSA assumes the team will spend 2 weeks developing the implementation plan; therefore, the time burden for this task will be five individuals x 40 hours x 2 weeks, or 400 hours. TSA uses a fully-loaded, blended wage rate of $93.64[10] to estimate a cost for this task to be $3,200,067. This is a one-time collection, and is depicted in Table 1.

**Table 1: Costs for Cybersecurity Implementation Plan (Mandatory - NEW)**

| Activity | Number of Responses | Time Burden per Response | Time Burden | Time Burden Cost |
|---|---|---|---|---|
| | A | B | C = A x B | D = C x $93.64 |
| Cybersecurity Implementation Plan | 73 | 400 | 29,200 | $3,200,067 |

**Cybersecurity Audit Plan:** TSA estimates 73 entities will conduct annual audits of their cybersecurity measures, and the time burden for submitting an annual audit plan to TSA is 40

[9] TSA newly-designated critical railroads will be subject to SD 1580-21-01.

[10] TSA calculates a blended wage rate for a team consisting of a cybersecurity manager and four cybersecurity analysts. TSA uses the unloaded rate for computer and information systems managers to represent the cybersecurity manager rate, which is $73.25. BLS. May 2021 National Industry-Specific Occupational Employment and Wage Estimates. NAICS 482000 –Rail Transportation. OCC 11-3021 Computer and Information Systems Managers. Last modified March 31, 2022 (accessed August 4, 2022). https://www.bls.gov/oes/2021/May/naics3_486000.htm. .
TSA uses the unloaded rate for information security analysts to represent cybersecurity analyst rate, which is $59.92. BLS. May 2021 National Industry-Specific Occupational Employment and Wage Estimates. NAICS 482000 – Rail Transportation. OCC 15-1211 Computer Systems Analysts. Last modified March 31, 2022 (accessed August 4,2022). https://www.bls.gov/oes/2021/May/naics3_486000.htm. The unloaded, blended rate = ($73.25 x 0.2) + ($59.92 x 0.8) = $62.59. The fully-loaded wage rate is $62.59 x 1.4961276 = $93.64.

hours. TSA believes the preparation and submission of the plan to TSA will be conducted by a corporate Audit/Compliance Manager, and uses a fully-loaded wage rate of $94.20.[11] The annual cost for this requirement is depicted in Table 2.

**Table 2: Annual Costs for Cybersecurity Audit Plans of Cybersecurity Measures (Mandatory - NEW)**

| Activity | Number of Annual Responses | Hour Burden per Response | Annual Hour Burden | Annual Hour Burden Cost |
|---|---|---|---|---|
| | A | B | C = A x B | D = C x $94.20 |
| Cybersecurity Audit Plan | 73 | 40 | 2,920 | $275,064 |

**Compliance Documentation:** TSA estimates 73 entities will conduct cybersecurity compliance documentation, and the time burden for this requirement is 80 hours. TSA believes this task will be performed by the cybersecurity manager, and applies a fully-loaded wage rate of $109.59. The annual cost for this requirement is depicted in Table 3.

**Table 3: Annual Costs for Compliance Documentation (Mandatory - NEW)**

| Activity | Number of Annual Responses | Hour Burden per Response | Annual Hour Burden | Annual Hour Burden Cost |
|---|---|---|---|---|
| | A | B | C = A x B | D = C x $109.59 |
| Compliance Documentation | 73 | 80 | 5,840 | $640,006 |

The total time burden of this NEW information collection for the 73 entities regulated under SD Rail-1580/1582-2022-01 is 29,200 (one-time) + 2,920 (annually) + 5,840 (annually) = 37,960 hours in Year 1, 8760 hours in Year 2, and 8760 in Year 3. This information is depicted in Table 4.

**Table 4: Total Costs**

| | Time Burden (in Hours) | Time Burden Cost |
|---|---|---|
| Year 1 | 37,960 | $4,115,137 |
| Year 2 | 8,760 | $915,070 |
| Year 3 | 8,760 | $915,070 |
| **Total** | **55,480** | **$5,945,276** |
| Average | 18,493 | $1,981,758.71 |

***SD Rail-1580-21-01, SD Rail-1582-21-01, and IC 2021-01 Series Collection:***

TSA estimates this collection applies to 457 railroad Owner/Operators, 115 rail transit system Owner/Operators, and 209 OTRB Owner/Operators, for a total of 781 respondents. Higher-risk railroad and rail transit Owner/Operators within the 781 respondents are required to provide Cybersecurity Coordinator information, complete a Cybersecurity Incident

[11] The unloaded wage rate for Administrative Services Managers is $62.96. BLS. May 2021 National Industry-Specific Occupational Employment and Wage Estimates. NAICS 482000 - Rail Transportation. OCC 11-3012 Administrative Services Managers. Last modified March 31, 2021 (accessed July 25,2022). https://www.bls.gov/oes/2021/May/naics3_486000.htm. TSA multiplies this rate by the load factor of 1.4961276, so $62.96 x 1.4961276 = $94.20.

Response Plan, complete and submit to TSA a Cybersecurity Vulnerability Assessment, and report cybersecurity incidents to CISA. Although the collections are voluntary for some respondents,[12] burden calculations assume all of the respondents will do all of the collections. TSA assumes these tasks will be performed by the cybersecurity coordinator, applies a fully-loaded wage rate of $109.59[13] for railroad cybersecurity coordinators, and $97.44[14] for rail transit system and for OTRB[15] cybersecurity coordinators.

Designate a Cybersecurity Coordinator/Alternate Cybersecurity Coordinator.
TSA estimates respondents will spend 1 hour each performing this task. Tables 5-7 represent the hour burden and hour burden cost for railroad Owner/Operators, rail transit system Owner/Operators, and OTRB Owner/Operators, respectively.

[12] Higher-risk OTRB and bus-only transit Owner/Operators received an IC that recommends they provide cybersecurity coordinator information, complete a Cybersecurity Contingency Plan, and report cybersecurity incidents. TSA also provides the IC to all respondents, recommending a Cybersecurity Assessment be completed.

[13] The unloaded wage rate for a Computer and Information Systems Manager is $73.25. BLS. May 2021 National Industry-Specific Occupational Employment and Wage Estimates. NAICS 482000 – Rail Transportation. OCC 11-3021 Computer and Information Systems Manager. Last modified March 31, 2022 (accessed August 4, 2021). https://www.bls.gov/oes/2021/May/naics3_482000.htm.
TSA calculates a load factor to increase the unloaded wage to account for non-wage compensation. TSA calculates this factor by dividing the total compensation ($32.84) by the wage and salary component ($21.95) of compensation to get a load factor of 1.4961276. BLS. Employer Costs for Employee Compensation – March 2022. Table 2. Employer costs per hour worked for employee compensation and costs as a percent of total compensation: private industry workers. Transportation and material moving occupations. Last modified June 16, 2022 (accessed August 4, 2022). https://www.bls.gov/news.release/archives/ecec_06162022.htm. TSA calculates a fully-loaded wage rate of $73.25 × 1.4961276 = $109.59.

[14] The unloaded wage rate for a Computer and Information Systems Manager is $65.13. BLS. May 2021 National Industry-Specific Occupational Employment and Wage Estimates. NAICS 485000 – Transit and Ground Transportation. OCC 11-3021 Computer and Information Systems Manager. Last modified March 31, 2022 (accessed August 4, 2022). https://www.bls.gov/oes/2021/May/naics3_485000.htm.
TSA uses the same load factor of 1.4961276 as described in the previous footnote to calculate a fully-loaded wage rate of $65.13 × 1.4961276 = $97.44.

[15] IC is recommended for OTRB operators are recommended the IC.

**Table 5: Hour Burden Cost for Freight Railroad Cybersecurity Coordinator and Alternate Information**

| Mode | Number of Responses | Hours per Response | Total Annual Hour Burden | Year 1 Hour Burden Cost |
|---|---|---|---|---|
| | A | B | C = A x B | D = C x $109.59 |
| FR | 457 | 1 | 457 | $50,083 |

**Table 6: Hour Burden Cost for Passenger Rail Transit Cybersecurity Coordinator and Alternate Information**

| Mode | Number of Responses | Hours per Response | Total Annual Hour Burden | Year 1 Hour Burden Cost |
|---|---|---|---|---|
| | A | B | C = A x B | D = C x $97.44 |
| PR | 115 | 1 | 115 | $11,206 |

**Table 7: Hour Burden Cost for OTRB Cybersecurity Coordinator and Alternate Information**

| Mode | Number of Responses | Hours per Response | Total Annual Hour Burden | Year 1 Hour Burden Cost |
|---|---|---|---|---|
| | A | B | C = A x B | D = C x $97.44 |
| OTRB | 209 | 1 | 209 | $20,365 |

In addition, TSA estimates that 50 respondents will need to update their cybersecurity coordinator and alternate information annually in both Year 2 and Year 3. The hour burden for Years 2 and 3 is 50 hours each, and the hour burden cost for Years 2 and 3 is $5,228[16] each.

Develop a Cybersecurity Incident Response Plan.

TSA estimates respondents will spend 80 hours each performing this task. Tables 8-10 represent the hour burden and hour burden cost for railroad Owner/Operators, rail transit system Owner/Operators, and OTRB Owner/Operators, respectively.

[16] TSA estimates that 58.51 percent (457 ÷ 781) of updated cybersecurity coordinator information in Years 2 and 3 will be from Railroad respondents, while the remainder (41.49 percent) will be from Rail Transit and OTRB respondents. Therefore, the hour burden cost of 50 respondents in years 2 and 3 is (50 × $109.61 × .5851) + (50 × $116.47 × .4149) = $5,622.81.

**Table 8: Freight Railroad Cybersecurity Incident Response Plan Development**

| Mode | Number of Responses | Hours per Response | Total Annual Hour Burden | Annual Hour Burden Cost |
|---|---|---|---|---|
| | A | B | C = A x B | D = C x $109.59 |
| FR | 457 | 80 | 36,560 | $4,006,660 |

**Table 9: Passenger Rail Transit Cybersecurity Incident Response Plan Development**

| Mode | Number of Responses | Hours per Response | Total Annual Hour Burden | Annual Hour Burden Cost |
|---|---|---|---|---|
| | A | B | C = A x B | D = C x $97.44 |
| PR | 115 | 80 | 9,200 | $1,008,240 |

**Table 10: OTRB Cybersecurity Incident Response Plan Development**

| Mode | Number of Responses | Hours per Response | Total Annual Hour Burden | Annual Hour Burden Cost |
|---|---|---|---|---|
| | A | B | C = A x B | D = C x $97.44 |
| OTRB | 209 | 80 | 16,720 | $1,629,243 |

Complete a Cybersecurity Vulnerability Assessment.
TSA estimates each respondent will spend an average of 42 hours performing this task. Tables 11-13 represent the hour burden and hour burden cost for railroad Owner/Operators, rail transit system Owner/Operators, and OTRB Owner/Operators, respectively.

**Table 11: Railroad Cybersecurity Vulnerability Assessment**

| Mode | Number of Responses | Hours per Response | Total Annual Hour Burden | Annual Hour Burden Cost |
|---|---|---|---|---|
| | A | B | C = A x B | D = C x $109.59 |
| FR | 457 | 42 | 19,194 | $2,103,496 |

**Table 12: Passenger Rail Transit Cybersecurity Vulnerability Assessment**

| Mode | Number of Responses | Hours per Response | Total Annual Hour Burden | Annual Hour Burden Cost |
|---|---|---|---|---|
| | A | B | C = A x B | D = C x $97.44 |
| PR | 115 | 42 | 4,830 | $470,649 |

**Table 13: OTRB Cybersecurity Vulnerability Assessment**

| Mode | Number of Responses | Hours per Response | Total Annual Hour Burden | Annual Hour Burden Cost |
|---|---|---|---|---|
| | A | B | C = A x B | D = C x $97.44 |
| OTRB | 209 | 42 | 8,778 | $855,353 |

Report cybersecurity incidents to CISA.
This burden is covered in OMB control number 1670-0037.

TSA estimates the total hour burden for the collection, relating to SD Rail-1580-01, SD Rail-1582-01, and IC 2021-01, to be 342,207 hours (134,023 hours in Year 1, 104,092 hours in Year 2, and 104,092 hours in Year 3), and total hour burden cost to be $35,922,818 ($14,158,602 in Year 1, $10,882,108 in Year 2, and $10,882,108 in Year 3). Table 14 represents the total hour burden and hour burden cost for this collection.

**Table 14: Summary Time Burden and Cost**

| IC Title | Responses | Hours per Response | Year 1 | | Year 2 | | Year 3 | |
|---|---|---|---|---|---|---|---|---|
| | | | Time Burden | Cost | Time Burden | Cost | Time Burden | Cost |
| Cybersecurity Implementation Plan | 73 | 400 | 29,200 | $3,200,067 | 0 | $0 | 0 | $0 |
| Annual Plan for Cybersecurity Assessment Program (Audit Plan) | 73 | 40 | 2,920 | $275,064 | 2,920 | $275,064 | 2,920 | $275,064 |
| Compliance Documentation | 73 | 80 | 5,840 | $640,006 | 5840 | $640,006 | 5,840 | $640,006 |
| Designation of Cybersecurity Coordinator | 781 | 1 | 781 | $81,654 | 50 | $5,228 | 50 | $5,228 |
| Cybersecurity Incident Response Plan | 781 | 80 | 62,480 | $6,532,377 | 62,480 | $6,532,377 | 62,480 | $6,532,377 |
| Cybersecurity Vulnerability Assessment | 781 | 42 | 32,802 | $3,429,434 | 32,802 | $3,429,434 | 32,802 | $3,429,434 |
| Total | 2,562 | | 134,023 | $14,158,602 | 104,092 | $10,882,108 | 104,092 | $10,882,108 |

***13. Provide an estimate of the total annual cost burden to respondents or recordkeepers resulting from the collection of information).***

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.***

***SD 1580/1582-22-01 Series Collection:***

For SD 1580/1582-2022-01 there are three elements of the mandatory collection on which TSA conducts reviews and audits and table & summaries these costs in Table 15.

**Table 15: TSA Hour Burden and Costs**

| Activity | Hour Burden | Wage Rate | First-Year Hour Burden Cost | Year-2 Hour Burden Cost | Year-3 Hour Burden Cost |
|---|---|---|---|---|---|
| | A | B | C = A x B | C = A x B | C = A x B |
| TSA Review of Implementation Plans (One-Time) | 2,336 | $90.88 | $212,302 | $0 | $0 |
| TSA Compliance Inspection | 3,504 | $73.95 | $259,121 | $259,121 | $259,121 |
| TSA Travel Costs for Compliance Inspections | | | $299,300 | $299,300 | $299,300 |
| TSA Review of Audit Plan | 292 | $73.95 | $21,593 | $21,593 | $21,593 |
| **Total** | | | **$792,316** | **$580,014** | **$580,014** |

**Cybersecurity Implementation Plan Reviews:** TSA estimates it will conduct 73 Cybersecurity Implementation Plan reviews utilizing a manager and an analyst. This is a one-time review, and the manager will spend 8 hours conducting the review, while the analyst will spend 24 hours. TSA uses a K-band rate of $102.20 for the manager and J-band rate of $87.11 for the analyst. The total cost of implementation plan reviews is 73 x ((8 hours x $102.20) + (24 hours x $87.11)) = $212,302.

**Compliance Inspections:** TSA estimates it will conduct 73 compliance inspections utilizing two inspectors. Each inspector will spend 24 hours each per inspection, so the total time burden for this activity will be 48 x 73 = 3,504 hours. TSA uses an I-band rate of $73.95 for the inspectors. The labor cost of compliance reviews is $73.95 x 3,504 = $259,121. In addition, TSA expects to spend $299,300 per year in travel costs; therefore, the total annual cost for compliance reviews is $558,421.

**Audit Plan Reviews:** TSA estimates it will conduct 73 Audit Plan reviews annually, and it takes an inspector 4 hours to conduct the review. TSA uses an I-band rate of $73.95 for the inspector. The total cost of audit plan reviews is 73 x 4 hours x $73.95 = $21,593.

TSA Time Burden: 10,001.4 hours (3,333.8 average per year)
TSA Cost: $1,957,017 ($652,339 average per year)

***SD 1580-21-01, SD 1582-21-01, and IC 2021-01 Collection:***
TSA estimates that it will receive and process 781 cybersecurity coordinator and alternate cybersecurity coordinator Point of Contact (POC) submissions in Year 1, and 50 submissions each in Years 2 and 3. TSA estimates it takes 5 minutes (0.08333 hour) to process each submission, and that it will be processed by an H-Band[17] (GS-12) pay level employee at TSA.

The government burden for this task during the 3-year period of analysis is 73 hours (average of 24.47 hours per year), and the burden cost is $4,673 (average $1,558 per year). [18]

The government burden and cost are displayed in Table 16.

**Table 16: Federal Government Time Burden and Cost**

| Type of Information Reported | Year 1 Responses | Year 2 Responses | Year 3 Responses | Hour Burden Per Response | Hour Burden | Total Hour Burden Cost |
|---|---|---|---|---|---|---|
| | A | B | C | D | E = (A+B+C) × D | F = E × $63.65 |
| Cybersecurity POC Info Processing | 781 | 50 | 50 | 0.08333 | 73 | $4,673 |
| Total | 781 | 50 | 50 | | 73 | $4,673 |

The total government time burden for this information collection is 10,001.4 hours + 73 hours = 10,075.1 hours (3,358.4 hours per year). The total government time burden cost is $1,957,017 + $4,674 = $1,961,690 ($653,897 per year).

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

TSA is making program changes as a result of the new collections to be implemented upon issuance of SD 1580/1582-2022-01.

***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.***

***SD 1580/1582-22-01 Series Collection***:
Regarding the new collection, no information resulting from the collections under the SD 1580/1582-2022-01will be published. However, TSA and CISA may use information submitted for vulnerability identification, trend analysis, or to generate anonymized

[17] The fully-loaded pay rate for an H-Band is $63.65. Source: TSA. Office of Finance and Administration, Personnel Modular Cost Data (FY21).
[18] The government burden for cybersecurity incident reports is reported in OMB control number 1670-0037.

indicators of compromise or other cybersecurity products to prevent other cybersecurity incidents.

***SD 1580-21-01, SD 1582-21-01, and IC 2021-01 Series Collection***:
Security information collected during the provision of Cybersecurity Coordinator information, Cybersecurity Incident Reporting, provision of the Cybersecurity Incident Response Plan and completion of the Cybersecurity Vulnerability Assessment will not be published. To the extent information collected via this process is considered to be SSI, it will be protected from disclosure and publication, and will be handled as described in 49 CFR part 1520.

***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.