INFORMATION COLLECTION SUPPORTING STATEMENT

Cybersecurity Measures for Surface Modes
OMB control number 1652-NEW
Exp.: xx/xx/2022

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).***

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." *See* 49 U.S.C. 114(d). In addition to carrying out the security responsibilities in paragraph (d), TSA is responsible for "assess[ing] threats to transportation" and "develop[ing] policies, strategies, and plans for dealing with threats to transportation security." *See* 49 U.S.C. 114(f)(3) and (4). 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). Under 49 U.S.C. 114(m), TSA may, at the discretion of the Administrator, assist another Federal agency, such as the Department of Homeland Security's Cybersecurity & Infrastructure Security Agency (CISA), in carrying out its authority in order to address a threat to transportation. Finally, TSA may issue security directives (SD) without prior notice and an opportunity to comment in order to protect transportation security. *See* 49 U.S.C. 114(l)(2).

On July 28, 2021, the White House issued a National Security Memorandum (NSM) on Improving Cybersecurity for Critical Infrastructure Control Systems, stating:

> The cybersecurity threats posed to the systems that control and operate the critical infrastructure on which we all depend are among the most significant and growing issues confronting our Nation. The degradation, destruction, or malfunction of systems that control this infrastructure could cause significant harm to the national and economic security of the United States.

The President's Industrial Control System Cybersecurity Initiative (Initiative) creates a path for Government and industry to collaborate to take immediate action, within their respective spheres of control, to address these serious threats.[1]

Cybersecurity incidents affecting surface transportation are a growing and dynamically evolving threat. Malicious cyber actors continue to target U.S. critical infrastructure, to include freight railroads, passenger railroads, and rail transit systems, with multiple cyberattack and cyber espionage campaigns. The United States' adversaries and strategic

[1] https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/

competitors will continue to use cyber espionage and cyberattacks to seek political, economic, and military advantage over the United States and its allies and partners.

The following recent ransomware attacks against this sector underscores this threat:

- July 2021: A cyberattack began to affect many small and medium-size business across the United States beginning Friday, and the attack was felt in Butte County, specifically on its bus system. The Butte Regional Transit's B-Line bus system serves Chico, Paradise, Magalia, Oroville, Palermo, Gridley and Biggs. It also has a paratransit offering for those with Americans with Disabilities Act certification or a "dial-a-ride" service for those 70 years and older[2].

- August 14, 2021: Cyberattack on Iran's railroad system last month caused widespread chaos with hundreds of trains delayed or canceled. The message itself was the work of the hackers and, in a sardonic twist, it advised confused travelers to seek more information by calling 64411 (New York Times).

- September 2021: The U.S. Cybersecurity and Infrastructure Security Agency (CISA) issued an alert on the increased use of Conti ransomware in more than 400 attacks on U.S. and international organizations. The alert comes after ransomware attacks on two major farming cooperatives, Crystal Valley Cooperative and New Cooperative — where the hacker asked for $5.9 million in payment.

To address this threat, TSA is issuing security directives to impose measures intended to enhance the security of these transportation systems from the impact of a cybersecurity attack. The transportation systems covered by the SDs and this Information Collection Request (ICR) are critical to U.S. national and economic security in that significant disruptions caused by a cyberattack could jeopardize the safety of passengers on these systems and quickly cause a ripple effect to other economic sectors that depend on rail transportation for materials and to carry goods to market.

Cyber attackers have demonstrated their willingness to conduct cyber-attacks against critical infrastructure by exploiting the vulnerability of Internet-accessible Operational Technology (OT) and Information Technology (IT) systems and assets. Given the multitude of connected devices already in use by the surface transportation industry and the vast amount of data generated (with more coming online soon), protecting the higher-risk freight rail, passenger rail, and rail transit industry has become an increasing critically important and complex undertaking to protect critical infrastructure from malicious cyber-attack and other cybersecurity-related threats.

To protect against the ongoing cybersecurity threat[3], TSA is issuing two SDs that mandate TSA-specified owner/operators of "higher risk" railroads and rail transit implement an array

[2] https://www.chicoer.com/2021/07/08/butte-county-bus-system-hit-by-weekend-cyberattack/

[3] TSA issued two SDs, effective May 28, 2021 and July 26, 2021, to enhance pipeline cybersecurity directly following the Colonial Pipeline Company's ransomware attack which lead to a disruption of critical supplies of gasoline and other refined petroleum products throughout the East Coast.

of cybersecurity measures to prevent disruption and degradation to their infrastructure.[4] The scope of these SDs align with the railroads and rail transit systems required to report significant security incidents to TSA under section 1570.203 of title 49, Code of Federal Regulations (CFR). For owner/operators not specifically covered under SDs 1580-2021-01 or 1582-2021-02, TSA is also issuing an "information circular" (IC), which are non-binding recommendations with the same measures. The requirements in the SD and the recommendations in the IC will allow TSA to execute its security responsibilities within the surface transportation industry, through awareness of potential security incidents and suspicious activities. The SDs will require, and the IC will recommend, that railroad owner/operators, rail transit system owner/operators, and over-the-road bus (OTRB) owner/operators conduct the following security measures:

1. Designate a Cybersecurity Coordinator who is required to be available to TSA 24/7 to coordinate cybersecurity practices and address any incidents that arise.
2. Report cybersecurity incidents to CISA.[5]
3. Develop a cybersecurity incident response plan to address cybersecurity gaps.
4. Complete a cybersecurity vulnerability assessment using the form provided by TSA.

Emergency Request

As noted above, TSA has statutory authority to immediately issue SDs if the TSA Administrator determines that actions are needed to protect transportation security. *See* 49 U.S.C. 114(*l*)(2). TSA is issuing two new SDs: SD 1580-2021-01, Enhancing Rail Cybersecurity, and SD 1582-2021-02, Enhancing Public Transportation and Passenger Railroads, to address the ongoing, serious threat. These SDs are being issued in coordination with CISA. In addition, TSA is preparing to issue an IC: IC-2021-01, Enhancing Surface Transportation Cybersecurity. The SDs secure "higher-risk" railroads and rail transit operations from cyber-attacks and addresses the continued threat to surface transportation security demonstrated by the ransomware attack on Colonial Pipeline and the incidents noted above. Since the Colonial incident, malicious actors have continued to successfully conduct ransomware attacks with a significant effect across the global supply chain. The IC recommends actions to enhance the security of these operations from the impact of cyberattacks. Impacts to applicable smaller operations could be even more significant due to their lack of available resources and inability to reconstitute after an attack. Recovery for this population would be challenging, so it is even more important that they follow the recommendations in the IC.

The required/recommended measures in TSA's SDs and IC are consistent with the functions and categories found in the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, which outlines security measures and controls intended to serve as a standard and best practices to assist organizations in managing cybersecurity risks and to promote the protection of critical infrastructure, as well as recommended measures in advisories issued by CISA.

[4] Agencies that are identified as higher-risk service the regions with the highest surface transportation-specific risk. Risk ranking is based on considerations related to ridership, location of services provided (use of the same stations and stops), and relationship between feeder and primary systems. *See* https://www.tsa.gov/sites/default/files/guidance-docs/high_threat_urban_area_htua_group_designations_0.pdf

[5] OMB control number 1670-0037 covers voluntary reporting to CISA through the US-CERT website.

To protect against the ongoing cybersecurity threat, the two SDs mandate that TSA-specified Owner/Operators of “Higher Risk” Railroads and Rail Transit implement an array of cybersecurity measures to prevent disruption and degradation to their infrastructure. In order to execute its security responsibilities within the surface transportation industry, TSA needs to have current awareness of potential security incidents and suspicious activity within the mode, so the IC recommends the same measures as the SDs.

TSA is seeking emergency approval of this new collection due to the need to impose additional emergency requirements for certain owner/operator through the issuance of SDs and to recommend cybersecurity measures for other owner/operators through the issuance of the IC.

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.***

TSA, in conjunction with federal partners such as the CISA, will use the reports of cybersecurity incidents to evaluate and respond to imminent and evolving cybersecurity incidents and threats as they occur. This monitoring will allow TSA and federal partners to take action to contain threats, take mitigating action, and issue timely warning to similarly situated entities against further spread of the threat. TSA and federal partners will also use the information to inform timely modifications to cybersecurity requirements to improve the security of the transportation security and the national economic security. TSA will use the collection of information to ensure compliance with TSA’s required cybersecurity measures by the SDs and the recommendations under the IC.

The following provides more detail on the measures included in the SDs and IC:

Designate a Cybersecurity Coordinator	Owner/Operators will be required or recommended, as applicable, to appoint a U.S. Citizen Cybersecurity Primary and Alternate Coordinator who must submit contact information. The Cybersecurity Coordinator serves as the primary contact for cyber-related intelligence information and cybersecurity-related activities and communications with TSA and CISA; must be accessible to TSA and CISA 24 hours a day, seven days a week; must coordinate cyber and related security practices and procedures internally; and must work with appropriate law enforcement and emergency response agencies.
Cybersecurity Incident Reporting	Owner/Operators Cybersecurity Coordinators will be required or recommended, as applicable, to report actual and potential cybersecurity incidents to CISA within 24 hours of identification of a cybersecurity incident. The information provided to CISA pursuant to the SD is shared with TSA and may also be shared with the National Response Center (NRC) and other agencies as appropriate. Conversely, information provided to TSA pursuant to this directive is shared with CISA and may also be shared with the NRC and other agencies as appropriate. 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.
Cybersecurity Contingency/Response Plan	Owner/Operators will be required or recommended, as applicable, to develop and adopt a Cybersecurity Incident Response Plan to reduce the risk of operational disruption should their Information and/or OT systems be affected by a cybersecurity incident. Owner/operators must provide or recommended to provide, as applicable, evidence of compliance to TSA upon request.
Cybersecurity Vulnerability Assessment	Owner/Operators will be required or recommended, as applicable, to assess their current cybersecurity posture consistent with the functions and categories found in the NIST Cybersecurity Guidance Framework. The assessment and identification of cybersecurity gaps must be completed using a using a form provided by TSA. As part of this assessment, the owners and operators must/may identify remediation measures to address the vulnerabilities and cybersecurity gaps identified during the assessment and a plan for implementing the identified measures if necessary, and report the results to TSA. TSA will use the results of the assessments to make a global assessment of the cyber risk posture of the industry and possibly impose additional security measures as appropriate or necessary. TSA may also use the information, with company-specific data redacted, for TSA's intelligence-derived reports. TSA and CISA may also use information submitted for vulnerability identification, trend analysis, or to generate anonymized indicators of compromise or other cybersecurity products to prevent other cybersecurity incidents. All reported information will be protected in a manner appropriate for the sensitivity and criticality of the information.

Certification of completion of SD requirements

Within 7 days of the deadlines set forth in the SD, owner/operators must ensure that their Cybersecurity Coordinator or other accountable executive submits a statement to TSA via email certifying that the owner/operator has met the requirements of the SD. Owner/Operators can complete and submit via email or other electronic options provided by TSA to submit the optional TSA forms (TSA SD-1580-2021-01: Statement of Completion and TSA SD-1582-2021-02: Statement of Completion) for each submission deadline. Documentation of compliance must be provided upon request. As the measures in the IC is voluntary, the IC will not contain this reporting requirement.

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. CISA has an approved information collection for cybersecurity incident reporting. *See* OMB control number 1670-0037.

For those owner/operators to whom the SD applies, they can submit statements confirming that they have complied with requirements within the established deadlines via e-mail. For convenience, TSA will also provide optional forms that can be submitted via email confirming completion (TSA SD-1580-2021-01 Statement of Completion and TSA SD-1582-2021-02 Statement of Completion) for each submission deadline.

In addition, owner/operators are required by the SD, and recommended under the IC, to develop a cybersecurity contingency/recovery plan to address cybersecurity gaps. Lastly, owner/operators required by the SD, and recommended under the IC to conduct the assessment of their cybersecurity posture using a TSA form and submit the results to TSA. There are two methods for owner/operators to submit the required information, which are considered Sensitive Security Information 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.

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.***

TSA works closely with its partners at the U.S. Department of Transportation's (DOT) Freight Rail Administration (FRA), Federal Transit Administration, and Federal Motor Carrier Safety Administration (FMCSA) to coordinate security initiatives. Since 2004, the two agencies have operated under an annex to the memorandum of understanding (MOU) between DOT and the Department of Homeland Security. This annex specifically addresses the respective roles and responsibilities of TSA and DOT as well as coordination processes. 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.

TSA coordinates closely with CISA which advances the Initiative's effort and secure the cybersecurity posture of the critical surface transportation sectors due to the interconnect 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, FRA, FTA, and FMCSA and other agencies as applicable. TSA requires reporting of certain information directly to CISA, which CISA will share with TSA to reduce duplication. Apart from the required (SDs) or encouraged (IC) reporting to CISA 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 SDs.

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.***

The SDs and IC apply to TSA identified owner/operators. This collection of information impacts a substantial number of small businesses because the requirement for OTRB operators who transport passengers through high-threat urban areas (HTUAs) may choose to report a cybersecurity incidents are generally small to medium size operators. Regarding the application of the IC, DHS determined that it is necessary to recommend these measures rather than requiring them due to the lower risk. The SDs primarily focus on the risk of a cyberattack against critical infrastructure that exploits the vulnerability of Internet-accessible OT and IT systems/assets. Buses, however, generally operate outside of an integrated rail network and are not as susceptible to significant impacts as a result of this type of cyberattack.

In addition, owner/operators are required by the SD, and recommended under the IC, to develop a cybersecurity contingency/recovery plan to address cybersecurity gaps.

The purpose of this plan is to reduce the impact of a cybersecurity incident, such as a ransomware attack. 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 supply chain.

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 emergency approval, DHS will be unable to address the critical, imminent threat of cyberattacks, such as ransomware, to the nation’s surface transportation systems. The use of normal PRA clearance procedures is reasonably likely to result in public harm because 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 operations and infrastructure to cybersecurity threats is fundamental to securing our nation’s travelling public and economic security. The cybersecurity incident information is covered under OMB control 1670-0037.

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 will be conducted consistent with the information collection guidelines, except for those in 5 CFR 1320.5(d)(2)(i), which 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. Owner/Operators are required by the SD, and recommended under the IC, to develop a cybersecurity contingency/recovery plan to address cybersecurity gaps.

   Owner/operators report cybersecurity incident information as soon as practicable, or for those required no later than 24 hours after a cybersecurity incident is discovered, or within 24 hours of recognition of a potential cybersecurity incident. This information collection is covered under OMB control number 1670-0037.

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 is currently seeking emergency approval of this collection. In light of the ongoing cybersecurity threat, TSA is seeking a waiver to the requirement in 5 CFR 1320.13(d) to publish a Federal Register notice announcing TSA is seeking emergency processing of this ICR. Upon approval of the Emergency Request, TSA will seek public comment on the collection following the normal clearance process providing a 60 and 30 Day commenting period. No waiver is required for the cybersecurity reporting incidents information collection, which is covered under OMB control number 1670-0037.

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 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 Sensitive Security Information 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 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; 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).

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 will be posed during the information collection.

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

TSA estimates this collection applies to 457 railroad owner/operators, 115 rail transit system owner/operators, and 209 over-the-road bus (OTRB) owner/operators, for a total of 781 respondents. "Higher risk" rail road and rail transit owner/operators within the 781 respondents will be required to provide cybersecurity coordinator information, complete a Cybersecurity Contingency Plan, and report cybersecurity incidents. Although the collections are voluntary for some respondents,[6] 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 $109.61[7] for railroad cybersecurity coordinators, and $116.47[8] for rail transit system and OTRB cybersecurity coordinators.

[6] "Higher Risk" OTRB and bus-only transit owner/operators will receive an IC that recommends they provide cybersecurity coordinator information, complete a Cybersecurity Contingency Plan, and report cybersecurity incident. TSA also provides the IC to all respondents, recommending a Cybersecurity Assessment be completed.

[7] The unloaded wage rate for a Computer and Information Systems Manager is $73.20. BLS. May 2020 National Industry-Specific Occupational Employment and Wage Estimates. NAICS 482000 – Rail Transportation. OCC 11-3021 Computer and Information Systems Manager. Last modified March 31, 2021 (accessed October 19, 2021). https://www.bls.gov/oes/2020/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 ($32.42) by the wage and salary component ($21.65) of compensation to get a load factor of 1.497459584. BLS. Employer Costs for Employee Compensation - June 2021. 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 September 16, 2021 (accessed October 19, 2021). https://www.bls.gov/news.release/archives/ecec_09162021.htm. TSA calculates a fully-loaded wage rate of $73.20 × 1.497459584 = $109.61.

[8] The unloaded wage rate for a Computer and Information Systems Manager is $77.78. BLS. May 2020 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, 2021 (accessed October 19, 2021). https://www.bls.gov/oes/2020/May/naics3_485000.htm.
TSA uses the same load factor of 1.497459584 as described in the previous footnote to calculate a fully-loaded wage rate of $77.78 × 1.497459584 = $116.47.

Designate a Cybersecurity Coordinator.

TSA estimates respondents will spend 1 hour each performing this task. Tables 1-3 represent the hour burden and hour burden cost for railroad owner/operators, rail transit system owner/operators, and OTRB owner/operators, respectively.

Table 1: Hour Burden Cost for Railroad Cybersecurity Coordinator Information

Number of Responses	**Hours per Response**	**Total Annual Hour Burden**	**Year 1 Hour Burden Cost**
A	**B**	**C = A x B**	**D = C x $109.61**
457	1	457	$50,094

Table 2: Hour Burden Cost for Rail Transit Cybersecurity Coordinator Information

Number of Responses	**Hours per Response**	**Total Annual Hour Burden**	**Year 1 Hour Burden Cost**
A	**B**	**C = A x B**	**D = C x $116.47**
115	1	115	$13,394

Table 3: Hour Burden Cost for OTRB Cybersecurity Coordinator Information

Number of Responses	**Hours per Response**	**Total Annual Hour Burden**	**Year 1 Hour Burden Cost**
A	**B**	**C = A x B**	**D = C x $116.47**
209	1	209	$24,343

In addition, TSA estimates that 50 respondents will need to update their cybersecurity coordinator 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 $5,623[9] each.

Develop a cybersecurity contingency/recovery plan.

TSA estimates respondents will spend 80 hours each performing this task. Tables 4-6 represent the hour burden and hour burden cost for railroad owner/operators, rail transit system owner/operators, and OTRB owner/operators, respectively.

[9] 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 4: Railroad Cybersecurity Contingency/Recovery Plan Development

Number of Responses	Hours per Response	Total Annual Hour Burden	Annual Hour Burden Cost
A	**B**	**C = A x B**	**D = C x $109.61**
457	80	36,560	$4,007,489

Table 5: Rail Transit Cybersecurity Contingency/Recovery Plan Development

Number of Responses	Hours per Response	Total Annual Hour Burden	Annual Hour Burden Cost
A	**B**	**C = A x B**	**D = C x $116.47**
115	80	9,200	$1,071,546

Table 6: OTRB Cybersecurity Contingency/Recovery Plan Development

Number of Responses	Hours per Response	Total Annual Hour Burden	Annual Hour Burden Cost
A	**B**	**C = A x B**	**D = C x $116.47**
209	80	16,720	$1,947,419

<u>Complete a cybersecurity vulnerability assessment.</u>
TSA estimates each respondent will spend an average of 42 hours performing this task. Tables 7-9 represent the hour burden and hour burden cost for railroad owner/operators, rail transit system owner/operators, and OTRB owner/operators, respectively.

Table 7: Railroad Cybersecurity Assessment

Number of Responses	Hours per Response	Total Annual Hour Burden	Annual Hour Burden Cost
A	**B**	**C = A x B**	**D = C x $109.61**
457	42	19,194	$2,103,932

Table 8: Rail Transit Cybersecurity Assessment

Number of Responses	Hours per Response	Total Annual Hour Burden	Annual Hour Burden Cost
A	**B**	**C = A x B**	**D = C x $116.47**
115	42	4,830	$562,562

Table 9: OTRB Cybersecurity Assessment

Number of Responses	Hours per Response	Total Annual Hour Burden	Annual Hour Burden Cost
A	**B**	**C = A x B**	**D = C x $116.47**
209	42	8,778	$1,022,395

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

TSA estimates the total hour burden for this collection to be 96,163 hours (96,063 hours in Year 1, 50 hours in Year 2, and 50 hours in Year 3), and total hour burden cost to be $10,814,420 ($10,803,173 in Year 1, $5,623 in Year 2, and $5,623 in Year 3). TSA has included the burden for the certification of completion within the burden numbers of each of the information collections.

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.

The government burden for cybersecurity incident reports is reported in OMB control number 1670-0037.

TSA estimates that it will receive and process 781 cybersecurity coordinator 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[10] (GS-12) pay level employee at TSA.

The total government burden during the 3-year period of analysis is 73 hours (average of 24.47 hours per year), and the burden cost is $3,173 (average $1,058 per year).

The government burden and cost are displayed in Table 10.

Table 10: 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 × $43.21**
Cybersecurity POC Info Processing	781	50	50	0.08333	73	$3,173
Total	781	50	50		73	$3,173

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

This is a new collection so there are no program changes.

[10] The fully-loaded pay rate for an H-Band is $43.21. Source: TSA. Office of Finance and Administration, Personnel Modular Cost Data (FY21).

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.***

    Security information collected during the provision of Cybersecurity Coordinator information, Cybersecurity Incident Reporting, provision of the Cybersecurity Contingency/Recovery Plans, and completion of the Cybersecurity Assessment will not be published or shared. 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 parts 15 and 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.