INFORMATION COLLECTION SUPPORTING STATEMENT

Cybersecurity Measures for Surface Modes
OMB control number 1652-0074
Exp.: 05/31/2022

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).

Congress granted the TSA Administrator broad statutory responsibility and authority with respect to the security of the transportation system.[1] Under the 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).

On July 28, 2021, the White House issued a National Security Memorandum 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.

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] *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 (SDs) 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 (ATSA), 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."

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.

To address this threat, on December 2, 2021, TSA issued Security Directive (SD) 1580-21-01 and SD 1582-21-02 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 SDs 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 over-the-road bus owner/operators not specifically covered under SDs 1580-21-01 or 1582-21-02. The requirements in the SDs 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.

On November 30, 2021, OMB approved TSA's request for an emergency approval of this collection to address the ongoing cybersecurity threat to surface transportation and associated infrastructure. The OMB approval allowed for the institution of mandatory reporting requirements under the SDs and collection of information voluntarily submitted under the IC. *See* ICR Reference Number: 202111-1652-003. TSA is now seeking renewal of this information collection for the maximum three-year approval period.

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 SDs require, and the IC recommends, the following security measures:

1. Designate a Cybersecurity Coordinator and alternate Cybersecurity Coordinator and provide contact information to TSA; these individuals are to be available to TSA 24/7 to coordinate cybersecurity practices, address any incidents that arise, and serve as a principal point of contact with TSA and the Cybersecurity and Infrastructure Security Agency (CISA) for cybersecurity-related matters;
2. Report cybersecurity incidents to CISA;
3. Develop a cybersecurity incident response plan to reduce the risk of operational disruption should an owner/operator's Information and/or Operational Technology systems be affected by a cybersecurity incident; and
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, uses 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 allows 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 also uses the information to inform timely

modifications to cybersecurity requirements to improve transportation security and national economic security. TSA uses the collection of information to ensure compliance with TSA's cybersecurity measures required by the SDs and the recommendations under the IC. Table 1 provides more detail on the measures included in the SDs and IC.

Table 1. Summary of Security Measures in the Security Directive and Information Circular

Title	Security Measure
Designate a Cybersecurity Coordinator	Owner/Operators are required or recommended, as applicable, to appoint a U.S. Citizen Cybersecurity Primary and at least one Alternate Coordinator; the Owner/Operator must or should, as applicable, 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/should be accessible to TSA and CISA 24 hours a day, seven days a week; must/should coordinate cyber and related security practices and procedures internally; and must/should work with appropriate law enforcement and emergency response agencies.
Cybersecurity Incident Reporting	Owner/Operators Cybersecurity Coordinators are 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/IC is shared with TSA and may also be shared with the National Response Center and other agencies as appropriate. Conversely, information provided to TSA pursuant to this directive/IC is shared with CISA and may also be shared with the National Response Center 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 Incident Response Plan	Owner/Operators are required or recommended, as applicable, to develop and adopt a Cybersecurity Incident Response Plan to reduce the risk of operational disruption should their Information Technology and/or Operational Technology systems be affected by a cybersecurity incident. Owner/Operators must provide or are recommended to provide, as applicable, evidence of compliance to TSA upon request.
Cybersecurity Vulnerability Assessment	Owner/Operators are required or recommended, as applicable, to assess their current cybersecurity posture consistent with the functions and categories found in the National Institute of Standards and Technology Cybersecurity Guidance Framework. The assessment and identification of cybersecurity gaps must or should, as applicable, 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 uses 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

The SDs and IC took effect on December 31, 2021. Owner/Operators must ensure within 7 days of the effective date of the SDs that they provide their designated Cybersecurity Coordinator information; within 90 days of the effective date of the SDs Owner/Operators must complete the Vulnerability Assessment (TSA form); within 180 days of the effective date of the SDs, Owner/Operators must adopt a Cybersecurity Incident Response Plan; within 7 days of completing the Cybersecurity Incident Response Plan requirement, Owner/Operators must submit a statement to TSA via email certifying that the owner/operator has completed this requirement of the SD. 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.

Portions of the responses that 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 15 and 1520.

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 or other electronic options provided by TSA. For convenience, TSA provides 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 are 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 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.

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.

The Department of Homeland Security (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 (FRA), Federal Transit Administration (FTA), and Federal Motor Carrier Safety Administration (FMCSA) 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, FRA, FTA, and FMCSA 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 SD 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 SDs 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.

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 over-the-road bus (OTRB) Owner/Operators who transport passengers through high-threat urban areas that may choose to report a cybersecurity incidents are generally small to medium size Owner/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 information 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.

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 operations and infrastructure to cybersecurity threats is fundamental to securing our nation's travelling 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).

This collection is 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.

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.

As required by 5 CFR 1320.8(d), TSA published a 60-day notice soliciting comments in the *Federal Register* on December 23, 2021 (86 FR 72988), and a 30-day notice on April 7, 2022 (87 FR 20453). No comments were submitted to TSA in response to the notices.

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

No payment or gift are 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 (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; 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 are 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 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 Contingency Plan, and report cybersecurity incidents. Although the collections are voluntary for some respondents,[3] 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[4] for railroad cybersecurity coordinators, and $116.47[5] for rail transit system and OTRB cybersecurity coordinators.

<u>Designate a Cybersecurity Coordinator/Alternate Cybersecurity Coordinator.</u>
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.

---

[3] "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.

[4] 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.

[5] 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.

Table 1: Hour Burden Cost for Railroad Cybersecurity Coordinator and Alternate 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 and Alternate 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 and Alternate 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 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 $5,623[6] 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.

[6] 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	$1,071,524

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	$1,947,378

Complete a cybersecurity vulnerability assessment.
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	$2,103,854

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	$562,550

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	$1,022,374

Report cybersecurity incidents to CISA.
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.

TSA estimates that it will receive and process 781 cybersecurity coordinator and alternate 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[7] (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). [8]

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	$3,154
Total	781	50	50		73	$3,154

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 renewal of an existing collection; there are no program changes.

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

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

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. 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.