

INFORMATION COLLECTION SUPPORTING STATEMENT

BASELINE ASSESSMENT FOR SECURITY ENHANCEMENT (BASE) PROGRAM

1652-0062

Exp.: 5/31/2024

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).***

Under the Aviation and Transportation Security Act¹ and delegated authority from the Secretary of Homeland Security, TSA has broad responsibility and authority for “security in all modes of transportation ... including security responsibilities ... over modes of transportation that are exercised by the Department of Transportation.”² In exercising its authority, TSA can assess threats to transportation; develop policies, strategies, and plans for dealing with threats to transportation security; and inspect, maintain, and test security facilities, equipment, and systems.³ For example, consistent with this authority, TSA is the Federal agency responsible for “assess[ing] the security of each surface transportation mode and evaluat[ing] the effectiveness and efficiency of current Federal Government surface transportation security initiatives.” Executive Order (E.O.) 13416, section 3(a) (Dec. 5, 2006). While many surface transportation entities have security and emergency response plans or protocols in place, no single database of this information exists, nor is there a consistent approach to evaluating the extent to which security and emergency response plans and protocols are in place across the surface transportation domain.

TSA has exercised its authority to assess threats to transportation through the Baseline Assessment for Security Enhancement (BASE) program, which provides a domain awareness, prevention, and protection program in support of TSA’s and the Department of Homeland Security’s (DHS) missions. TSA initially developed the BASE program for public transportation systems to evaluate the status of security and emergency response procedures throughout the nation and, because of the program’s success, expanded it into the highway transportation domain.⁴ The BASE program is a completely voluntary program, with no penalties for declining to participate, or for not having any voluntary security elements in place. Specifically, a BASE review assesses the security measures of a transportation system and gathers data used by TSA to address its responsibilities, such as evaluating “effectiveness and efficiency of current Federal Government surface transportation security initiatives” and developing modal specific annexes to the

¹ Pub. L. 107-71 (115 Stat. 597; Nov. 19, 2001), as codified at 49 U.S.C. 114.

² 49 U.S.C. § 114(d).

³ 49 U.S.C. § 114(f).

⁴ Previously, for highway transportation, TSA exercised its assessment authority through Corporate Security Reviews (CSRs) with organizations engaged in transportation by motor vehicles and those that maintain or operate key physical assets within the highway transportation community (DISCONTINUED TSA OMB control number 1652-0036). TSA consolidated these assessment programs within surface modes of transportation under the BASE program, TSA OMB control number 1652-0062.

Transportation Systems Sector Specific Plan⁵ that include “an identification of existing security guidelines and requirements and any security gaps...” E.O. 13416, Sec. 3(c)(i).

This information collection request (ICR) also covers collections of information required by the “Gerardo Hernandez Airport Security Act of 2015” (Hernandez Act).⁶ This Act, named after a TSA employee killed while on duty by an active shooter in 2013, requires TSA to gather specific information from passenger transportation agencies and providers with high-risk facilities, regarding incident response plans for active shooters, acts of terrorism, or other security-related incidents that target passengers. TSA is also required to disseminate best practices for security incident planning, management, and training and to establish a mechanism through which to share such practices with passenger transportation agencies nationwide.

The Government Accountability Office (GAO), audit GAO-20-404, “Passenger Rail Security: TSA Engages with Stakeholders but Could Better Identify and Share Standards and Key Practices (April 2020),” recommended TSA update the BASE cybersecurity questions to ensure they reflect key practices.⁷ TSA concurred with the GAO’s recommendation and is revising the collection to include questions that cover all five functions of the National Institute of Standards and Technology (NIST) cybersecurity framework, which include Identify, Protect, Detect, Response and Recover. All core functions and a majority of the subcategories are integrated with industry best practices in the newly developed cybersecurity questions and cybersecurity annex questions, strengthening the cybersecurity health for the transportation sector.

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.*

BASE Reviews

TSA’s Surface Transportation Security Inspectors (TSIs) are trained to conduct BASE reviews during site visits with security and operating officials of affected transportation systems. These TSIs capture and document relevant information using a standardized electronic checklist. Advance coordination and planning ensures the efficiency and effectiveness of the assessment process. Stakeholders may also obtain a checklist in advance from TSA and conduct self-assessments of their security readiness.

A BASE review evaluates the surface transportation system’s security program components using a two-phased approach: (1) field collection of information, and (2) analysis/evaluation of collected information. The information collected by TSA through BASE reviews strengthens the security of evaluated surface transportation systems by supporting security program development (including grant programs), and the analysis/evaluation provides a

⁵ Transportation System Sector-Specific Plan is a planning tool for Transportation Sector Agencies, critical infrastructure owners and operators, and partners at the regional, State, local, tribal, and territorial levels that guides and integrates efforts to secure and strengthen the resilience of critical infrastructure, identifies the Transportation Sector’s security and resilience priorities, and describes the approach to managing critical infrastructure risk.

⁶ Pub. L. 114-50 (129 Stat. 490; Sept. 24, 2015).

⁷ Additional information regarding this audit and the GAO’s recommendations are available on the GAO’s website using the audit number (GAO-20-0404) or at the following link: <https://www.gao.gov/products/gao-20-404>.

consistent road map for stakeholders to improve their security and emergency programs vulnerabilities. TSA provides all surface transportation systems that undergo a BASE review with a comprehensive report of results that can be used to prioritize identified vulnerabilities to enhance security. The report includes a score derived from the checklist, which is comprised of security action item categories with multiple questions that are weighted. Each security action item category is averaged for an overall score.

As part of the new data collection requirements triggered by the GAO recommendations, TSA is revising the information collection to add 21 questions to both BASE assessments. The questions relate to an entities' cybersecurity program. The previous versions did not include the Detect and Recover functions of the NIST framework. TSA has determined it is necessary to request the stakeholders to provide this additional information in order to fully implement the GAO's recommendations. The impact to the stakeholders will be minimal and consistent with the purposes of the BASE and uses of information, including allowing TSA to assess and share best practices with the same stakeholder community.

Specifically, the information collected will be used as follows:

1. To develop a baseline understanding of a transportation system's security and emergency management processes, procedures, policies, and activities against security requirements and recommended security practices issued by TSA and the Department of Transportation (DOT).
2. To enhance a transportation system's overall security posture through collaborative review and discussion of existing security activities, identification of areas of potential weakness or vulnerability, and development of remedial recommendations and courses of action.
3. To identify procedures and protocols implemented by a transportation system that represent an "effective" or "smart" security practice warranting the sharing of information across the relevant modal community to foster general enhancement of security.
4. To inform TSA's development of security strategies, priorities, and programs for the most effective application of available resources. In mass transit/passenger rail, the BASE is a supporting element for funding distributed under the Transit Security Grant Program.⁸

Cybersecurity Annex

Consistent with GAO's recommendation, TSA also developed a cybersecurity annex for the entities interested in a comprehensive, thorough assessment of their cybersecurity hygiene. The annex is voluntary and designed to complement the BASE program, but will be conducted independent of the BASE checklist. In adding the cybersecurity annex, TSA is revising the information collection by increasing the total number of questions to 87, where

⁸ The TSGP directly supports transportation infrastructure security activities, as appropriated by the Department of Homeland Security Appropriations Act, 2019 (Pub. L. No. 116-6; 133 Stat. 13; Feb. 15, 2019), and authorized by section 1406 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (Pub. L. No 110-53; 121 Stat. 266; Aug. 3, 2007), codified at 6 U.S.C. § 1135. The program provides funding to owners and operators of transit systems (which include intra-city bus, commuter bus, ferries, and all forms of passenger rail) to protect and increase the resilience of critical surface transportation infrastructure and the traveling public from acts of terrorism.

there are 21 BASE questions and 66 cybersecurity annex questions. This effort aligns with TSA's Cybersecurity Roadmap⁹ to gain a understanding of the national transportation cybersecurity posture, providing necessary information to assess and prioritize cybersecurity risks to the sector.

- 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. [Effective 03/22/01, your response must SPECIFICALLY reference the Government Paperwork Elimination Act (GPEA), which addresses electronic filing and recordkeeping, and what you are doing to adhere to it. You must explain how you will provide a fully electronic reporting option by October 2003, or an explanation of why this is not practicable.]**

The majority of the information collected relevant to a BASE review is through the site visit. During BASE reviews, TSA's Surface Transportation Security Inspectors receive and document relevant information through electronic means, utilizing an electronic checklist, in compliance with GPEA. The cybersecurity annex can be completed in conjunction with a regular BASE or as a standalone assessment.

- 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 actively monitors information collected by our Federal partners but has found no other collection that can meet the needs of the BASE program. TSA is sensitive to the burden on the industry from complying with requests for information and has taken appropriate steps to avoid overlap where possible. For example, during the development of the questions used in the BASE programs, TSA reached out to Cybersecurity and Infrastructure Security Agency (CISA) and received input from DOT and its modal administrations, as well as industry partners, through the Office of Security Policy and Industry Engagement's Peer Advisory Group.

There is no duplication with CISA. TSA values CISA's expertise, and our new cybersecurity annex is in alignment with CISA's expectations of where the surface transportation industry should be heading. TSA is adding questions based on the GAO audit, and the current waves of cyber attacks, such as ransomware demands that are frequently occurring in the surface transportation industry. TSA's adding these additional questions benefits CISA cybersecurity ongoing efforts.

While TSA is the lead Federal agency for security in all modes of transportation, TSA has limited the Highway BASE to non-hazardous materials carriers and shippers in order to avoid duplication with the Federal Motor Carrier Safety Administration assessments for compliance with requirements of the Pipeline and Hazardous Materials Safety

⁹ The TSA Cybersecurity Roadmap provides TSA with a framework directly aligned to the DHS Cybersecurity Strategy, by which TSA is to execute its cybersecurity responsibilities over the next five years.

https://www.tsa.gov/sites/default/files/documents/tsa_cybersecurity_roadmap_adm_approved.pdf

Administration. Similarly, TSA's BASE is distinct from Federal Transit Administration (FTA) assessments. The Federal Transit Administration focuses on mandatory safety standards while TSA focuses on security assessments.

Similar to the approach for recent BASE changes and developments, TSA obtained feedback from our transportation partners through the American Public Transportation Association, American Trucking Association, and the pupil transportation community on the new cybersecurity questions.

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.*

Although TSA plans to collect information from businesses of all sizes, there is minimal potential burden to small businesses or other small entities.

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.*

No single database of this information exists; nor is there a consistent approach to evaluating the extent to which security and emergency response plans and protocols are in place across the surface transportation domain. If this collection is not conducted, TSA will be unable to assess current security practices in the public transportation/passenger rail and highway transportation sectors, and will, therefore, be unable to fully exercise its oversight authority as provided for under 49 U.S.C. 114. If the information collection is conducted less frequently, TSA's ability to compare data collected at different sites will be diminished.

In general, the BASE program provides TSA with up-to-date information on current security practices within the public transportation/passenger rail and highway/motor carrier transportation sectors. This information allows TSA to adapt programs to the changing threat, while incorporating an understanding of the improvements owners/operators make in their security posture, whereas without this information the ability of TSA to perform its security mission would be severely hindered. Additionally, the relationships these face-to-face contacts foster are critical to the Federal Government's ability to quickly reach out to the affected transportation systems to respond to any incidents.

In its report on the audit GAO-20-404, the GAO noted that updating the BASE cybersecurity questions to align more closely with the core functions in the NIST Cybersecurity Framework is necessary for TSA to (1) better assist passenger rail and other operators in identifying current key practices and improving their cybersecurity posture; (2) ensure transit operators are more aware of cybersecurity vulnerabilities and better prepared to reduce the impact from a cybersecurity incident; and (3) create a more consistent cybersecurity approach from TSA.¹⁰ Further, without the additional cybersecurity questions, TSA would not have the necessary information to assess and prioritize cybersecurity risks to the sector.

¹⁰ *Supra* n. 7 at p 40-41.

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).

TSA will conduct this collection in a manner consistent with the general information collection guidelines in 5 CFR 1320.5(d)(2).

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

TSA invited public comment on this information collection requirement, a 60-day notice was published in the *Federal Register* on June 4, 2021 (86 FR 30065) and a 30-day notice was published on August 26, 2021 (86 FR 47653).

TSA received a comment on the 60-day notice from the Chemical Facility Security News blog, inquiring about the limited detail in the notice on TSA's burden estimate. TSA's more detailed calculations and explanations are included in this Information Collection Supporting Statement, which is available for public viewing upon submission to OMB. Based on historical BASE information, TSA is providing detailed burden estimates for Mass Transit and Passenger Rail (MT/PR) and Highway/Motor Carrier transportation systems in this document (see question 12).

The commenter inquired about the unavailability of the new cybersecurity questions. The ICR documentation, including the new cybersecurity questions, which was not finalized at the time the 60-day notice was published, will be available at <http://www.reginfo.gov> upon its submission to OMB.

Also, the commenter took issue with TSA not soliciting comments via the Federal eRulemaking Portal. TSA requests comments to the 60-day notice be sent to TSAPRA@tsa.dhs.gov. However, TSA routinely checks the Federal eRulemaking portal, <https://www.regulations.gov/document>, for additional comments, recognizing that the public has been using this additional vehicle. Further, for this collection, upon checking the Federal eRulemaking Portal at the close of the comment period, TSA found that one non-responsive comment was submitted to the portal for the BASE collection in response to the 60-day notice.

Finally, TSA appreciates the commenters suggestion that TSA mandate completion of the BASE cybersecurity annex; currently all TSA BASE reviews are voluntary.

TSA did not receive any comments on the 30-day notice.

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

TSA will not provide payment or gifts to respondents.

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

While TSA does not offer any assurance of confidentiality, portions of the information provided by respondents and the resulting BASE reviews are designated Sensitive Security Information (SSI), as determined by the TSA SSI Program Office, and are handled in accordance with 49 CFR 1520. In addition, this collection is covered by the Privacy Impact Assessment (PIA) for the DHS General Contact Lists. See, DHS/ALL/PIA-006, June 15, 2007.

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.

TSA does not ask questions of a private or sensitive nature.

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

TSA developed the BASE program for certain surface modes of transportation to evaluate the status of security and emergency response procedures throughout the nation. The BASE collection covers mass transit/passenger rail (MT/PR) and Highway/Motor Carrier transportation systems. The standard BASE collections are conducted by TSA's Surface TSIs during site visits with security and operating officials of transportation systems. TSA provides estimates of the hour burden costs due to these information collection activities.

TSA conducts approximately 75 assessments for MT/PR respondents annually. A MT/PR assessment takes approximately 12.5 hours. TSA estimates that it takes an additional 6 hours to complete the new cybersecurity annex, and that 50 percent of the MT/PR population will conduct the BASE Assessment with the cybersecurity annex, and 50 percent without the cybersecurity annex. This results in an MT/PR annual hour burden of 1,162.50 hours, or 3,487.50 hours over three years. To estimate costs, TSA uses a fully-loaded¹¹ wage rate of \$74.83 for MT/PR respondents.¹² TSA estimates an annual hour burden cost of \$86,989.12. for this collection, or \$260,967.37 over three years. Table 1 summarizes these calculations.

¹¹ A fully-loaded wage rate accounts for non-salary costs of employee compensation, such as health and retirement benefits.

¹² The unloaded wage rate for MT/PR General and Operations Managers is \$49.81. BLS. May 2020 National Industry-Specific Occupational Employment and Wage Estimates. NAICS 485000 - Transit and Ground Passenger Transportation. OCC 11-1021 General and Operations Managers. Last modified March 31, 2021 (accessed May 10, 2021), https://www.bls.gov/oes/2020/May/naics3_485000.htm. To estimate the loaded wage, TSA calculates a compensation factor to inflate the wage rate accounting for benefits. The compensation factor is 1.511704. BLS. Employer Costs for Employee Compensation – December 2020. Table 5. Employer costs per hour worked for employee compensation and costs as a percent of total compensation: private industry workers. Production, transportation and material moving occupations. Last modified March 18, 2021 (accessed May 10, 2021), https://www.bls.gov/news.release/archives/eccec_03182021.htm. The fully-loaded wage rate of \$ 74.83 is the product of the unloaded wage rate and the compensation factor.

INFORMATION COLLECTION SUPPORTING STATEMENT

BASELINE ASSESSMENT FOR SECURITY ENHANCEMENT (BASE) PROGRAM

**1652-0062
Exp.: 5/31/2024**

Table 1: MT/PR Respondents Hour Burden and Costs

	MT/PR Assessments per Year	Number of Entities Who Take Assessment W/O Cyber Annex	Hour Burden per Assessment W/O Cyber Annex	Hour Burden W/O Cyber Annex	Number of Entities Who Take Assessment With Cyber Annex	Hour Burden per Assessment With Cyber Annex	Hour Burden With Cyber Annex	Total Hour Burden	Total Hour Burden Cost
Year	A	B = A x 50%	C = 12.5 hours	D = B x C	E = A x 50%	F = C + 6 Hours	G = E x F	H = D + G	I = H x \$74.83
2021	75	37.5	12.50	468.75	37.50	18.5	693.8	1,162.5	\$86,989.12
2022	75	37.5		468.75	37.50		693.8	1,162.5	\$86,989.12
2023	75	37.5		468.75	37.50		693.8	1,162.5	\$86,989.12
Total	225.00			1,406.25			2081.25	3,487.50	\$260,967.37
Annual Average	75			468.75			693.75	1,162.50	\$86,989.12

Note: Totals may not add due to rounding.

INFORMATION COLLECTION SUPPORTING STATEMENT

BASELINE ASSESSMENT FOR SECURITY ENHANCEMENT (BASE) PROGRAM

1652-0062
Exp.: 5/31/2024

TSA conducts approximately 107 Highway/Motor Carrier assessments per year. A Highway/Motor Carrier assessment takes approximately 2 hours. TSA estimates it takes an additional 6 hours to complete the new cybersecurity annex, and that 50 percent of the Highway/Motor Carrier population will conduct the BASE Assessment with the Cybersecurity Annex, and 50 percent without the cybersecurity annex. This results in an annual hour burden of 535 hours, or 1,605 hours over 3 years. TSA uses a fully-loaded wage rate of \$80.06 for Highway/Motor Carrier respondents.¹³ TSA estimates an annual hour cost burden of \$42,832.02 for this collection, or \$128,496.06 over three years. Table 2 summarizes these calculations.

¹³ The unloaded wage rate for Highway General and Operations Managers is \$52.96. BLS. May 2020 National Industry-Specific Occupational Employment and Wage Estimates. NAICS 484000 - Truck Transportation. OCC 11-1021 General and Operations Managers. Last modified March 31, 2021 (accessed May 10, 2021), https://www.bls.gov/oes/2020/May/naics3_484000.htm. To estimate the loaded wage, TSA calculates a compensation factor to inflate the wage rate accounting for benefits. The compensation factor is 1.511704. BLS. Employer Costs for Employee Compensation – December 2020. Table 5. Employer costs per hour worked for employee compensation and costs as a percent of total compensation: private industry workers. Production, transportation and material moving occupations. Last modified March 18, 2021 (accessed May 10, 2021). https://www.bls.gov/news.release/archives/eccec_03182021.htm. The fully-loaded wage rate of \$80.06 is the product of the unloaded wage rate and the compensation factor.

INFORMATION COLLECTION SUPPORTING STATEMENT

BASELINE ASSESSMENT FOR SECURITY ENHANCEMENT (BASE) PROGRAM

**1652-0062
Exp.: 5/31/2024**

Table 2: Highway/Motor Carrier Respondents Hour Burden and Cost

	Assessments per Year	Number of Entities Who Take Assessment W/O Cyber Annex	Hour Burden per Assessment W/O Cyber Annex	Hour Burden W/O Cyber Annex	Number of Entities Who Take Assessment With Cyber Annex	Hour Burden per Assessment With Cyber Annex	Hour Burden With Cyber Annex	Total Hour Burden	Total Hour Burden Cost
Year	A	$B = A \times 50\%$	C = 2 hours	$D = B \times C$	$E = A \times 50\%$	$F = C + 6$ hours	$G = E \times F$	$H = D + G$	$I = H \times \$80.06$
2021	107	53.5	2	107	53.5	8	428	535	\$42,832.02
2022	107	53.5		107	53.5		428	535	\$42,832.02
2023	107	53.5		107	53.5		428	535	\$42,832.02
Total	321.0			321			1284	1605	\$128,496.06
Annual Average	107.0			107			428	535	\$42,832.02

Note: Totals may not add due to rounding.

INFORMATION COLLECTION SUPPORTING STATEMENT

**BASELINE ASSESSMENT FOR SECURITY ENHANCEMENT (BASE)
PROGRAM**

1652-0062

Exp.: 5/31/2024

The total respondents for these assessments are $75 + 107 = 182$ respondents per year, or 546 respondents over three years. The total hour burden to the public is $1,162.50$ hours + 535 hours = $1,697.5$ hours per year, or $5,092.50$ hours over three years. The total hour burden cost to the public is $\$86,969.12 + \$42,832.02 = \$129,821.14$ per year, or $\$389,463.43$ over three years.

INFORMATION COLLECTION SUPPORTING STATEMENT

**BASELINE ASSESSMENT FOR SECURITY ENHANCEMENT (BASE)
PROGRAM**

1652-0062
Exp.: 5/31/2024

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

There are no additional costs with this collection.

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 standard BASE collections are conducted by two TSIs during site visits. The total cost incurred by the Federal Government is the sum of TSIs' preparation, site visits assessment activity, data entry, and follow-up paperwork costs.

For each MT/PR assessment, 2 TSIs spend approximately 120 hours per site visit (60 hours per TSI): 20 hours for preparation, 80 hours of assessment activity, and 20 hours for data entry and follow-up. For each Highway/Motor Carrier assessment, 2 TSIs spend approximately 80 hours per site visit (40 hours per TSI): 20 hours for preparation, 40 hours of assessment activity, 20 hours for data entry and follow-up. TSA estimates an annual hour burden of 9,000 for MT/PR assessments and 8,560 for Highway/Motor Carrier assessments, for a total annual hour burden of 17,560 hours. TSA TSIs consist of H- and I-Band employees, with an average wage of \$57.97.¹⁴ TSA estimates an annual hour burden cost to TSA of \$1,017,953, or \$3,053,859.60 over 3 years. Table 3 summarizes this estimate.

Table 3: TSA Hour Burden and Costs

Activity	Assessments per Year	Hour Burden per Assessment	Annual Hour Burden	Annual Hour Burden Cost
	A	B	C = A × B	D = C × \$57.97
MT/PR Assessments	75	120	9,000	\$521,730.00
Highway Assessments	107	80	8,560	\$496,223.20
Total	182		17,560	\$1,017,953.20

Note: Totals may not add due to rounding.

¹⁴ An H Band employee earns an average of \$43.21 hourly and an I Band earns \$72.73 hourly, including benefits. TSA uses the average of the two hourly compensation rates.

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

As a result of the GAO report referenced above, TSA modified the cybersecurity section of the BASE. TSA added additional questions, resulting in an increase in the public hour burden. In addition, TSA developed the cybersecurity annex questions for stakeholders concerned about their cybersecurity posture, and who are opting for a cybersecurity in-depth review. These changes resulted in an increase in the public hour burden.

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.

TSA will not publish the results of this collection.

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.

TSA is not seeking such approval.

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

TSA is not seeking any exceptions to the statement in Item 19.