

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, the Transportation Security Administration (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 and motor carrier (HMC) 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

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 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.

Government surface transportation security initiatives” and developing modal specific annexes to the 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 also covers collections of information required by the “Gerardo Hernandez Airport Security Act of 2015” (Hernandez Act).⁶ The Hernandez 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 revised the collection to include questions that cover the five core 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 BASE (Cy-BASE) question sets, strengthening cybersecurity in 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 on 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

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>.

program development (including grant programs), and the analysis/evaluation provides a 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. Each security action item category is averaged for an overall score.

As part of the new data collection requirements triggered by the GAO-20-404 recommendations, TSA revised the information collection by adding 21 questions to each BASE type, and a stand-alone Cy-BASE. 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 stakeholders 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 BASE

Consistent with GAO's recommendation, TSA also developed a Cy-BASE for the entities interested in a comprehensive, thorough assessment of their cybersecurity program. The Cy-BASE is voluntary and designed to complement the BASE program and is conducted independent of the public transportation/passenger railroads (PTPR) and HMC BASE checklists. TSA revised the information collection by adding 87 cybersecurity questions,

⁸ The Transit Security Grant Program 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.

and from the 87, pulled 21 into to the BASEs security action item on cybersecurity. This effort aligns with TSA's Cybersecurity Roadmap⁹ to gain an 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 checklist is provided by the entity well before the onsite visit through routine electronic means. This allows the entity to provide necessary documentation prior to the first onsite visit when information on the TSIs checklist that is lacking or missing can be addressed with the entity. TSIs utilize an electronic checklist for the purpose of annotating their findings following their onsite visit and document reviews, in compliance with the GPEA. The Cy-BASE can be completed in conjunction with a regular BASE or as a standalone assessment.

TSA conducted a study on the usability of the BASE in 2024 to determine the accuracy of the estimated time burden to complete the collection, if it was easy to comprehend and if stakeholders understood the purpose and content of the BASE questions. The study included four participants; with all participants taking on the persona of stakeholders with little or no knowledge of the BASE. The average time to complete BASE questions was approximately 3 minutes, which corresponds to the current estimated time burden of 3.17 minutes. Applicants who needed time locating answers within their current cybersecurity plans and records, or time to confer with cybersecurity experts or cybersecurity contractors would need more time to completely provide accurate answers. Overall the participants found the questions clear and easy to understand, and felt the information they provided was necessary to determine if the participant's cybersecurity posture is optimal for protecting their cyber assets. The participants did not provide any recommendations for the improvement of the BASE and the study showed the annual burden is an accurate estimation. 9 hours per assessment, or 540 minutes, divide that by the 170 questions, is 3.17 minutes per question.

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 surface transportation related BASE program. TSA

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 5 years.

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

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 the Cybersecurity and Infrastructure Security Agency (CISA) and received input from DOT and its modal administrations, as well as industry partners, through the Policy, Plans and Engagement's Peer Advisory Group.

TSA values CISA's expertise, and our new Cy-BASE is in alignment with CISA's expectations of where the surface transportation industry should be heading. TSA added 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's ongoing cybersecurity efforts.

While TSA is the lead Federal agency for security in all modes of transportation, TSA has limited the HMC 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 Administration. Similarly, TSA's PTPR BASE is distinct from Federal Transit Administration 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 PTPR and HMC 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 PTPR and HMC 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 the BASE cybersecurity questions to align more closely with the core functions in the NIST Cybersecurity Framework and 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.

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 November 13, 2023, 88 FR 77602, and a 30-day notice was published on May 17, 2024, 89 FR 43421. TSA received no comments in response to the notices.

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

¹⁰ *Supra* n. 7 at p 40-41.

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 PTPR and HMC 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 70 assessments for PTPR respondents annually. A PTPR assessment takes approximately 9 hours. This results in an PTPR annual hour burden of 630 hours, or 1,890 hours over 3 years. To estimate costs, TSA uses a fully-loaded¹¹ wage rate of \$62.70 for PTPR respondents.¹² TSA estimates an annual hour burden cost of \$39,499. for this collection, or \$118,498 over 3 years. Table 1 summarizes these calculations.

Table 1: PTPR Assessment Respondents Hour Burden and Costs

	Assessments per Year	Hour Burden per Assessment	Total Hour Burden	Total Hour Burden Cost
Year	A	B	C = A × B	D = C × \$62.70
Year 1	70	9	630	\$39,499.29
Year 2	70		630	\$39,499.29
Year 3	70		630	\$39,499.29
Total	210		1,890	\$118,497.87
Annual Average	70		630	\$39,499.29

Note: Calculations may not add due to rounding.

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 PTPR General and Operations Managers is \$41.92. BLS. May 2022 National Industry-Specific Occupational Employment and Wage Estimates. NAICS 485000 - Transit and Ground Passenger Transportation. OCC 11-1021 General and Operations Managers. Last modified April 25, 2023 (accessed April 25, 2023), https://www.bls.gov/oes/2022/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 1.495641. BLS. Employer Costs for Employee Compensation – June 2023. 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 September 12, 2023 (accessed October 16, 2023), https://www.bls.gov/news.release/archives/eccec_09122023.htm. The fully-loaded wage rate of \$62.70 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

TSA conducts approximately 107 HMC assessments per year. An HMC assessment takes approximately 2 hours. This results in an annual hour burden of 193 hours, or 578 hours over 3 years. TSA uses a fully-loaded wage rate of \$66.89 for HMC respondents.¹³ TSA estimates an annual hour cost burden of \$12,882 for this collection, or \$38,646 over 3 years. Table 2 summarizes these calculations.

Table 2: Highway Assessment Respondents Hour Burden and Costs

Year	Assessments per Year	Hour Burden per Assessment	Total Hour Burden	Total Hour Burden Cost
	A	B	C = A × B	D = C × \$66.89
Year 1	107	1.8	192.6	\$12,882.07
Year 2	107		192.6	\$12,882.07
Year 3	107		192.6	\$12,882.07
Total	321		577.8	\$38,646.20
Annual Average	107		192.6	\$12,882.07

Note: Calculations may not add due to rounding.

¹³ The unloaded wage rate for HMC General and Operations Managers is \$44.72. BLS. May 2022 National Industry-Specific Occupational Employment and Wage Estimates. NAICS 484000 - Truck Transportation. OCC 11-1021 General and Operations Managers. Last modified April 25, 2023 (accessed April 25, 2023), https://www.bls.gov/oes/2022/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 1.49561. BLS. Employer Costs for Employee Compensation – June 2023. 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 September 12, 2023 (accessed October 16, 2023). https://www.bls.gov/news.release/archives/eccec_09122023.htm. The fully-loaded wage rate of \$66.89 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

TSA conducts approximately eight cybersecurity assessments per year. A cybersecurity assessment takes approximately 7.8 hours. This results in an annual hour burden of 62 hours, or 187 hours over 3 years. TSA uses a fully-loaded wage rate of \$64.79.¹⁴

Table 3: Cybersecurity Assessment Hour Burden and Cost

	Assessments per Year	Hour Burden per Assessment	Total Hour Burden	Total Hour Burden Cost
Year	A	B	C = A × B	D = C × \$64.79
Year 1	8	7.8	62.4	\$4,042.97
Year 2	8		62.4	\$4,042.97
Year 3	8		62.4	\$4,042.97
Total	24		187.2	\$12,128.91
Annual Average	8		62.4	\$4,042.97

Note: Calculations may not add due to rounding.

The total respondents for these assessments are $70 + 107 + 8 = 185$ respondents per year, or 555 respondents over 3 years. The total hour burden to the public is $630 \text{ hours} + 193 \text{ hours} + 62 \text{ hours} = 885 \text{ hours}$ per year, or 2,655 hours over 3 years. The total hour burden cost to the public is $\$39,499 + \$12,882 + \$4,043 = \$56,424$ per year, or \$169,273 over 3 years.

¹⁴ The wage rate is a blended, fully-loaded rate assuming 50 percent of cybersecurity assessments are conducted by PTPR entities and 50 percent by HMC entities.

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 PTPR assessment, two 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 HMC assessment, two 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 8,400 for PTPR assessments and 8,560 for HMC assessments, for a total annual hour burden of 16,960 hours. TSA TSIs consist of H- and I-Band employees, with an average wage rate of \$68.80.¹⁵ TSA estimates an annual hour burden cost to TSA of \$1,166,771, or \$3,500,313 over 3 years. Table 4 summarizes this estimate.

Table 4: 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 × \$68.80
MT/PR Assessments	70	120	8,400	\$577,881.80
Highway Assessments	107	80	8,560	\$588,889.07
Total	177		16,960	\$1,166,770.86

Note: Calculations may not add due to rounding.

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

¹⁵ An H Band employee earns an average of \$63.65 hourly and an I Band earns \$73.95 hourly, including benefits. TSA uses the average of the two hourly compensation rates (\$68.80).

TSA moved to a stand-alone Cy-BASE information collection by going from two Cybersecurity Assessment information collections (PTPR Cybersecurity and HMC Cybersecurity) to one Cybersecurity Assessment information collection. This resulted in a decrease in the cybersecurity respondents, going from 92 to 8 respondents, and a decrease in the public hour burden, moving from 1,122 to 62 annual hours. The respondents to the PTPR and HMC Assessments information collections increased from 92 to 177 respondents and the burden increased from 575 to 823 annual hours. As a result, the total respondents for the overall collection are 185 respondents and the total annual burden is 885 annual hours, decreasing from the previous 1,698 annual burden hours.

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.