



February 2024

SURFACE TRANSPORTATION THREATS

Better Communication
with Stakeholders
Needed about the
Security Clearance
Process

GAO Highlights

Highlights of [GAO-24-106382](#), a report to congressional committees

Why GAO Did This Study

The U.S. surface transportation system comprises multiple modes of transportation and moves billions of passengers and millions of tons of goods each year. The National Defense Authorization Act for Fiscal Year 2022 includes provisions for DHS to take steps to enhance surface transportation security through information sharing. Steps include allocating intelligence staff to locations with higher-risk assets and making security clearance applications available to surface transportation stakeholders. The act includes a provision for GAO to review implementation of these steps.

This report describes (1) how and where TSA and DHS I&A allocated field-based intelligence staff and (2) the extent to which DHS made the security clearance application process available to surface transportation stakeholders, among other topics. GAO analyzed TSA and DHS I&A documents and data, including staff allocations for fiscal year 2023, conducted site visits to areas with higher-risk surface transportation assets, and interviewed agency officials and surface transportation stakeholders.

What GAO Recommends

GAO recommends TSA, DHS I&A, and CISA implement communications approaches that convey consistent and accurate information about accessing the security clearance application process. DHS agreed with the recommendations.

View [GAO-24-106382](#). For more information, contact Triana McNeil at (202) 512-8777 or McNeilT@gao.gov.

February 2024

SURFACE TRANSPORTATION THREATS

Better Communication with Stakeholders Needed about the Security Clearance Process

What GAO Found

The Transportation Security Administration (TSA) and Department of Homeland Security's Office of Intelligence and Analysis (DHS I&A) allocated field-based intelligence staff to locations with higher-risk surface transportation assets. TSA and DHS I&A considered surface transportation security risks differently when doing so because each took into account their other mission priorities. Though their approaches differed, in fiscal year 2023, TSA and DHS I&A each allocated field-based intelligence staff to approximately half of the 62 geographic areas with higher-risk surface transportation assets. According to TSA and DHS I&A officials, the remaining locations with higher-risk surface transportation assets that did not have field-based intelligence staff located within the geographic area were supported by field-based intelligence staff in other locations.

Surface Transportation Modes



Sources: GAO analysis of Transportation Security Administration documents; photos (l to r) serjio74/Stock Adobe.com, vacant/Stock Adobe.com, Svetlaya/Stock Adobe.com, Tomasz Wozniak/stock.adobe.com. | GAO-24-106382

DHS made the security clearance application process available to surface transportation stakeholders, but some misunderstood aspects of the process. DHS and its entities—TSA, DHS I&A, and the Cybersecurity and Infrastructure Security Agency (CISA)—have applicable policies and other guidance. However, agency officials, field-based intelligence staff, and surface transportation stakeholders GAO interviewed misunderstood how some aspects were applied, specifically as they related to accessing the security clearance application process. For example, some misunderstood which DHS entity was responsible for initiating applications for surface transportation owners and operators, whether there was a maximum number each would sponsor, and the type of employee eligible. Implementing a coordinated communications approach could help ensure relevant agency staff, as well as surface transportation stakeholders, have consistent and accurate information about the security clearance application process and ultimately facilitate classified information sharing when the need arises. Each DHS entity is responsible for ensuring its own staff have accurate information about the security clearance process. Further, as the lead agency for sharing transportation security-related information, TSA would be best positioned to coordinate the communications approach for sharing information with surface transportation owners and operators and external stakeholders about accessing the security clearance application process.

Contents

Letter		1
	Background	5
	TSA and DHS I&A Used Different Approaches and Allocated Field-Based Intelligence Staff to Many Areas with Higher-Risk Surface Transportation Assets	15
	Field-Based Intelligence Staff and Other Public and Private Entities Participate in Information Sharing Activities Related to Surface Transportation Security	23
	TSA and DHS I&A Have Measures Intended to Protect Privacy, Civil Rights, and Civil Liberties When Sharing Information about Surface Transportation Security	31
	Surface Transportation Stakeholders Can Apply for Security Clearances through DHS, but Some Stakeholders and Agency Staff Had Misunderstandings about Some Aspects of Accessing the Process	38
	Conclusion	49
	Recommendations for Executive Action	50
	Agency Comments	51
Appendix I	Field-Based Intelligence Staffing in Locations with Higher-Risk Surface Transportation Assets for Fiscal Year 2023	53
Appendix II	Comments from the Department of Homeland Security	59
Appendix III	GAO Contact and Staff Acknowledgments	64
Tables		
	Table 1: Examples of Transportation Security Administration (TSA) and Department of Homeland Security Office of Intelligence and Analysis (DHS I&A) Intelligence and Information Products	14
	Table 2: Transportation Security Administration (TSA) Field-Based Intelligence Staff Allocation by Location Type for Fiscal Year 2023	20
	Table 3: Department of Homeland Security (DHS) Office of Intelligence and Analysis (I&A) Field-Based Intelligence Staff Allocation by Location Type for Fiscal Year 2023	22

Table 4: Summary of Fair Information Practice Principles	32
Table 5: Location and Type of Higher-Risk Surface Transportation Asset, Fiscal Year 2023	53
Table 6: Transportation Security Administration (TSA) and Department of Homeland Security (DHS) Office of Intelligence and Analysis (I&A) Staffing in Locations with Higher-Risk Surface Transportation Assets, by Location for Fiscal Year 2023	56

Figures

Figure 1: Higher-Risk Surface Transportation Assets by Mode, According to the Transportation Security Administration (TSA)	6
Figure 2: Locations with More Than One Higher-Risk Surface Transportation Asset, as Defined by the Transportation Security Administration in Fiscal Year 2023	9
Figure 3: Offices that Review Transportation Security Administration (TSA) and Department of Homeland Security (DHS) Office of Intelligence and Analysis (I&A) Finished Intelligence Products for Privacy, Civil Rights, and Civil Liberties Issues	36
Figure 4: Prior GAO Review of Department of Homeland Security's (DHS) Office of Intelligence and Analysis (I&A) Implementation of Civil Rights, Civil Liberties, and Privacy Protections	37
Figure 5: Number of Security Clearance Applications Initiated by the Transportation Security Administration (TSA) for Surface Transportation Owners and Operators, Fiscal Years 2018 through 2023	39
Figure 6: Transportation Security Administration (TSA) Process for Surface Transportation Stakeholders to Apply for a Security Clearance	43

Abbreviations

CISA	Cybersecurity and Infrastructure Security Agency
DHS	Department of Homeland Security
DHS I&A	DHS Office of Intelligence and Analysis
FBI	Federal Bureau of Investigation
SLTPS	state, local, tribal, and private sector
TSA	Transportation Security Administration

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



February 7, 2024

The Honorable Gary C. Peters
Chairman
The Honorable Rand Paul, M.D.
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Mark E. Green, M.D.
Chairman
The Honorable Bennie G. Thompson
Ranking Member
Committee on Homeland Security
House of Representatives

The U.S. surface transportation system moves billions of passengers and millions of tons of goods each year. It comprises multiple modes of transportation, including public transportation and passenger railroads, freight railroads, and over-the-road buses, as well as pipelines that transport natural gas and hazardous liquids like oil.¹ These types of assets have previously been the target of both terrorist acts and cyberattacks.²

Securing the surface transportation system is complicated by the number of public and private sector stakeholders involved in operating and protecting it. Given the number of stakeholders involved, timely and effective sharing of information about threats to surface transportation is necessary to secure the system. Within the federal government, the Department of Homeland Security's (DHS) Transportation Security Administration (TSA) has primary responsibility for securing all transportation modes—including surface transportation modes—and sharing information about threats to those modes.³ Other federal

¹Public transportation and passenger railroad service includes commuter rail, heavy and light rail, intercity rail, and mass transit buses. Over-the-road buses refer to motor vehicles with an elevated passenger deck located over a separate baggage area, as customarily used for intercity, commuter, and tour bus operations.

²We provide more information on these incidents later in this report.

³See generally 49 U.S.C. § 114(d), (f). The U.S. Coast Guard also plays a lead role in maritime transportation security. 6 U.S.C. § 468(a)(2).

stakeholders are involved, including DHS's Office of Intelligence and Analysis (DHS I&A), DHS's Cybersecurity and Infrastructure Security Agency (CISA), the Department of Transportation, and the Federal Bureau of Investigation (FBI). In addition, state and regional fusion centers and public and private owners and operators of surface transportation assets play a role.⁴

The National Defense Authorization Act for Fiscal Year 2022 directed DHS to take steps related to enhancing surface transportation security through information sharing.⁵ These steps included prioritizing the placement of TSA and DHS I&A field-based intelligence staff to locations with higher-risk surface transportation assets; sharing information in a manner that protects privacy, civil rights, and civil liberties; and making security clearance applications available to surface transportation owners and operators to foster sharing of classified information, when appropriate.⁶

The National Defense Authorization Act for Fiscal Year 2022 includes a provision for us to review DHS's implementation of these activities not later than 2 years after enactment.⁷ Specifically, our report:

1. describes how and where TSA and DHS I&A allocated field-based intelligence staff to locations with higher-risk surface transportation assets;
2. describes how TSA and DHS I&A field-based intelligence staff participate in information sharing activities related to surface transportation security;

⁴Fusion centers are state or local-run collaborative efforts that serve as a focal point for intelligence gathering, analysis, and sharing of threat information among federal, state, and local partners. The goal of fusion centers is to maximize the ability to detect, prevent, investigate, apprehend, and respond to criminal or terrorist activity. See 6 U.S.C. § 124h(k)(1).

⁵Pub. L. No. 117-81, § 6418, 135 Stat. 1541, 2415-2417 (2021).

⁶For the purposes of this document, field-based intelligence staff refers to TSA's field intelligence officers and DHS I&A's intelligence officers. Intelligence staff does not include other intelligence personnel, such as TSA's headquarters intelligence analysts or DHS I&A's field-based reports officers. While such personnel may play a role in generating intelligence products, they generally do not have direct relationships with surface transportation owners and operators.

⁷§ 6418(e), 135 Stat. at 2416.

-
3. describes the measures TSA and DHS I&A have to protect privacy, civil rights, and civil liberties when sharing information about threats to surface transportation assets; and
 4. assesses the extent to which DHS has made the security clearance application process available to owners and operators of surface transportation assets.

To address all four objectives, we (1) analyzed relevant documentation, (2) interviewed agency officials, (3) conducted site visits to gather information from field-based staff and surface transportation stakeholders, and (4) interviewed officials from associations representing surface transportation owners and operators.

- We analyzed laws, regulations, policies, guidance, and other documentation—including internal operating procedures and training materials—related to TSA and DHS I&A information sharing activities. For example, we analyzed laws related to DHS I&A's responsibilities, regulations used to define higher-risk surface transportation assets, and agency policies related to the security clearance application process. We also collected and reviewed TSA and DHS I&A intelligence and information products related to surface transportation security.
- We interviewed officials from several TSA, DHS I&A, and CISA offices. We discussed topics related to the allocation of field-based intelligence staff; the type and frequency of information sharing activities; measures in place to protect privacy, civil rights, and civil liberties; and the availability of security clearances, among other topics.
- We selected six locations with higher-risk surface transportation assets that included a range of higher-risk surface transportation modes and geographic dispersion.⁸ In each location, we conducted interviews either virtually or in person with TSA and DHS I&A field-based intelligence staff, TSA surface transportation inspectors, fusion

⁸The six locations we selected were the Chicago Area, Greater Los Angeles Area, Houston Area, Greater Washington, D.C./National Capital Region, New York City/Northern New Jersey Area, and Philadelphia Area. We selected locations that included a range of surface transportation modes and were geographically dispersed. Specifically, to select these locations, we analyzed the location of higher-risk surface transportation assets, fusion centers, and relevant TSA and DHS I&A staff. We also considered TSA's and DHS I&A's field structures to maximize our coverage of their respective regional organization.

center staff, and surface transportation owners and operators.⁹ We discussed topics related to the allocation of field-based intelligence staff; the type and frequency of information sharing activities; measures in place to protect privacy, civil rights, and civil liberties; and the availability of security clearances, among other topics. The information we obtained in these interviews is not generalizable but provides valuable insights from field-based staff and surface transportation stakeholders.

- We interviewed officials from five associations that represent surface transportation owners and operators and the association that represents fusion centers.¹⁰ We discussed topics related to the type and frequency of information sharing activities and the availability of security clearances for their members, among other topics.

In addition to activities related to all objectives, (1) for the first objective, we analyzed data to describe TSA's and DHS I&A's allocation of field-based intelligence staff for fiscal year 2023 relative to the location of higher-risk surface transportation assets, and (2) for the fourth objective, we evaluated the extent to which DHS made the security clearance application process available to surface transportation owners and operators. Following are further details on our methodology for those two objectives.

To address our first objective, TSA identified surface transportation assets it considers at higher risk of being targeted or used by terrorists, relative to other assets of the same transportation mode.¹¹ We used the TSA-provided information to identify the geographic areas where the assets were located and compared the locations to TSA and DHS I&A

⁹To ensure we collected the perspectives of major freight rail companies, which operate regional or nationwide systems through many of the selected locations but are headquartered elsewhere, we interviewed two freight railroad companies headquartered outside those locations. We did not interview a surface inspector aligned to the Greater Washington, D.C./National Capital Region.

¹⁰We selected the five associations representing surface transportation owners and operators to cover each of the surface transportation modes included in the definition of surface transportation. We selected two associations representing pipeline companies to include perspectives of both natural gas pipeline owners and operators, as well as those whose pipelines transport hazardous liquids. Specifically, we interviewed representatives from the Association of American Railroads, the American Bus Association, the American Public Transportation Association, the American Petroleum Institute, and the American Gas Association.

¹¹We provide the definitions of higher-risk surface transportation assets for each mode later in this report.

staff allocation data for fiscal year 2023 (the most recent fiscal year with complete data). We assessed these data by conducting logic tests and interviewing knowledgeable officials about their collection. We found the data sufficiently reliable for reporting the number and location of staff allocated and the number of positions that were vacant as of the end of fiscal year 2023. We also obtained and analyzed relevant TSA documentation to understand the extent to which the proximity of a higher-risk surface transportation asset is considered in staff assignments.¹²

To address our fourth objective, we analyzed the information collected from interviews with agency officials, field-based staff, surface transportation owners and operators, and relevant associations. We compared the information in those interviews to the applicable TSA and DHS I&A policies and processes for non-federal stakeholders to access the security clearance application process. We also evaluated the extent to which the content of those documents was consistent with communication principles described in GAO's Standards for Internal Control in the Federal Government.¹³

We conducted this performance audit from November 2022 to February 2024 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Higher-Risk Surface Transportation Assets

The U.S. surface transportation system is a complex system comprising multiple modes of transportation, such as public transportation and passenger railroads, freight railroads, and over-the-road buses, as well as pipelines that transport natural gas and hazardous liquids like oil. These modes are often interconnected and operate in close coordination with

¹²DHS I&A did not have relevant documentation because it did not consider the presence of higher-risk surface transportation assets in making decisions about staff allocations, as we discuss later in this report.

¹³GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington D.C.: Sep. 2014).

one another, to the point that the American economy and way of life heavily depend on this network operating securely and safely.

TSA does not have a singular definition or set of criteria for identifying “high-risk surface transportation assets.” According to TSA officials, it considers public transportation and passenger railroads, freight railroads, and over-the-road buses “higher-risk” if they meet the criteria identified in federal regulations. Specific criteria for what is considered higher-risk differ for each mode of transportation, but are used to identify operations with a relatively higher risk of being targeted or used by terrorists.¹⁴ For pipelines, TSA uses criteria, including the amount of throughput in the pipeline system and its use in other critical sectors, to determine if a pipeline is “critical,” and thus, higher-risk (see figure 1).

Figure 1: Higher-Risk Surface Transportation Assets by Mode, According to the Transportation Security Administration (TSA)



Public Transportation and Passenger Railroads^a

TSA identifies the public transportation systems and passenger railroad systems it considers to be higher risk in federal regulations.^b These higher-risk systems include 46 public transportation and passenger railroad systems in eight geographic areas centered around a metropolitan area, Amtrak, and owners or operators of systems that host a higher-risk freight or passenger rail operation.^c



Freight Railroads

TSA identifies the freight railroad systems it considers to be higher risk in federal regulations.^d These higher-risk freight railroads include Class I railroads, railroads that transport Rail Security-Sensitive Materials (e.g., explosives) in a High-Threat Urban Area, and railroads that host a higher-risk freight or passenger rail operation.^e As of the end of fiscal year 2023, there were 33 railroads TSA considered higher-risk—six Class I railroads and 27 railroads that met other parts of the definition.



Over-the-Road Buses

TSA identifies the over-the-road bus operations it considers to be higher in federal regulations.^f These operations provide fixed-route service to, from, or through any of 10 urban areas identified in those regulations.^g



Pipelines

TSA considers a pipeline higher risk if it is critical to the United States and its incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or a combination thereof. TSA identifies the critical pipeline systems based primarily on an assessment of the volume of material transported through the system in a year.^h

Source: GAO analysis of TSA information; photos (l to r, top to bottom) serjib74/Stock Adobe.com, vacant/Stock Adobe.com, Svetlaya/Stock Adobe.com, Tomasz Wozniak/Stock Adobe.com. | GAO-24-106382

Note: Specific criteria for what is considered higher-risk differs for each mode of transportation, but are used to identify operations with a relatively higher-risk of being targeted or used by terrorists. Security Training for Surface Transportation Employees, 85 Fed. Reg. 16,456 (Mar. 23, 2020)

¹⁴Security Training for Surface Transportation Employees, 85 Fed. Reg. 16,456 (Mar. 23, 2020) (describing a higher-risk operation as one that meets the criteria in 49 C.F.R. §§ 1582.101 (public transportation system and passenger railroads), 1580.101 (freight railroads), and 1584.101 (over-the-road buses)). Higher-risk operations are required to have a security program, as indicated by the Implementing Recommendations of the 9/11 Commission Act of 2007. Pub. L. No. 110-53, § 1408, 121 Stat. 266, 409 (codified at 6 U.S.C. § 1137).

(describing a higher-risk operation as one that meets the criteria in 49 C.F.R. §§ 1582.101 (public transportation system and passenger railroads), 1580.101 (freight railroads), and 1584.101 (over-the-road buses)). Higher-risk operations are required to have a security program, as indicated by the Implementing Recommendations of the 9/11 Commission Act of 2007. Pub. L. No. 110-53, § 1408, 121 Stat. 266, 409 (codified at 6 U.S.C. § 1137).

^aPublic transportation and passenger railroads may include multiple transportation types, including commuter rail, heavy and light rail, intercity rail, and mass transit buses.

^b49 C.F.R. § 1582.101; 85 Fed. Reg. 16,456, 16,458 (Mar. 23, 2020).

^cThe eight geographic areas are: Bay Area, CA; Greater Los Angeles Area, CA; Greater Washington, D.C./National Capital Region, DC/MD/VA; Atlanta Area, GA; Chicago Area, IL/IN; Boston Area, MA; New York City/Northern New Jersey Area, NY/NJ/CT; and Philadelphia Area, PA/NJ.

^d49 C.F.R. § 1580.101; 85 Fed. Reg. 16,456, 16,458 (March 23, 2020).

^eThe Surface Transportation Board categorizes freight railroads into three classes for regulatory purposes based on annual operating revenues. As of July 2023, Class I freight railroads are railroads that earn \$1.032 billion or more annually. As of September 2023, there were 6 Class I railroads including: BNSF Railway, CSX Transportation, Canadian National Railway, Canadian Pacific Kansas City Limited, Norfolk Southern Railway, and Union Pacific Railroad.

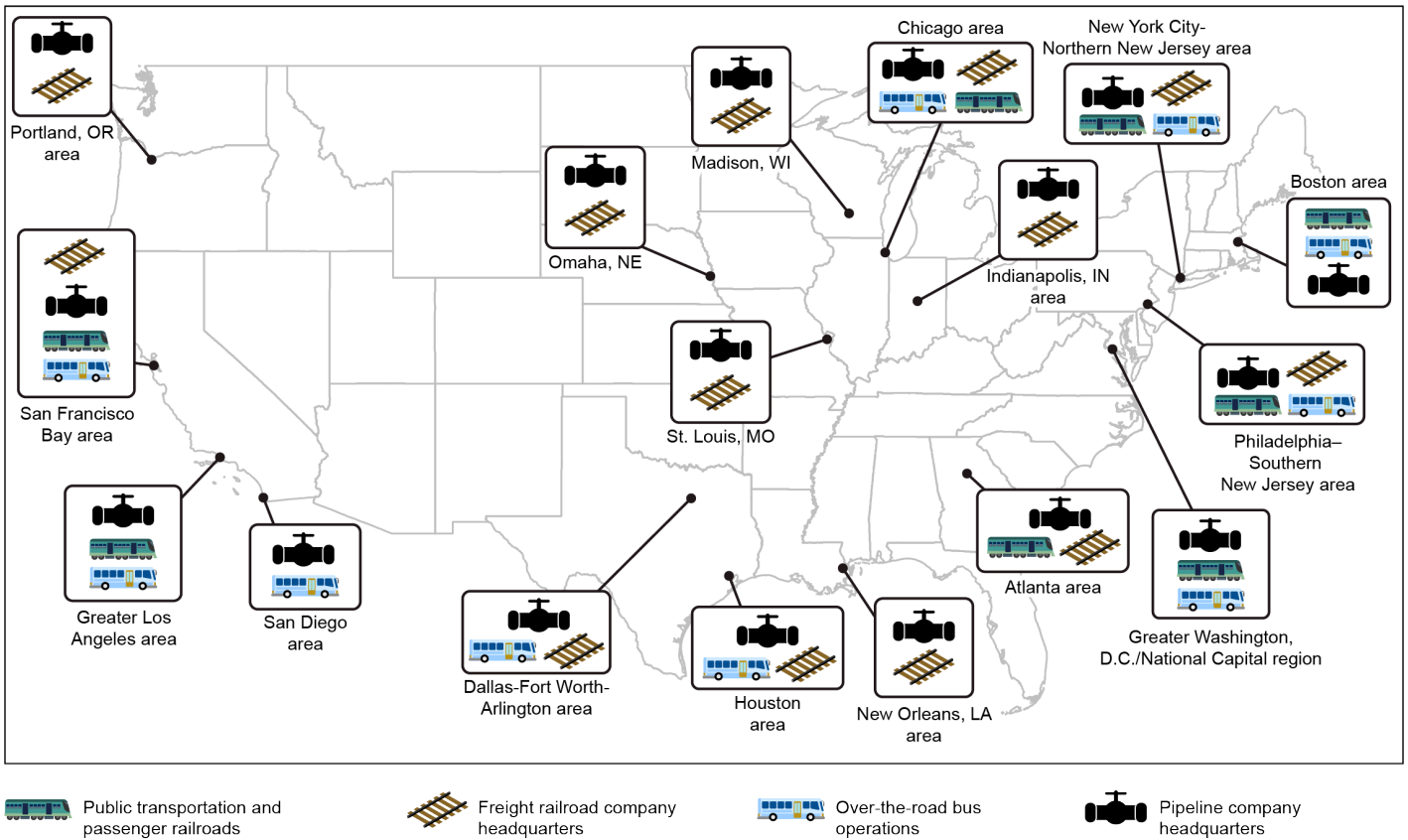
^f49 C.F.R. § 1584.101; 85 Fed. Reg. 16,456, 16,458 (March 23, 2020). An over-the-road bus is a motor vehicle with an elevated passenger deck located over a separate baggage area, as customarily used for intercity, commuter, and tour bus operations.

^gThe 10 areas are: Anaheim/Los Angeles/Long Beach/Santa Ana Areas, CA; San Diego Area, CA; San Francisco Bay Area, CA; Washington, D.C./National Capital Region, DC/VA/MD/WV; Chicago Area, IL/IN; Boston Area, MA; New York City/Jersey City/Newark Area, NY/NJ/PA; Philadelphia Area/Southern New Jersey Area, PA/DE/NJ; Dallas Fort Worth/Arlington Area, TX; and Houston Area, TX.

^hSome companies own or operate more than one critical pipeline system.

In fiscal year 2023, there were a total of 62 geographic areas with at least one higher-risk surface transportation asset—that is, a higher-risk public transportation and passenger railroad, over-the-road bus operations, or a freight railroad or pipeline company headquarters. According to TSA officials, the location of the headquarters of certain asset types whose systems span multiple states or regions is important because the company’s security staff with whom field-based intelligence staff generally coordinate are often headquarters-based. Having such staff located in the same geographic area as TSA or DHS I&A staff helps to facilitate information sharing, including classified information that is typically done in person. Seventeen of these geographic areas had more than one mode of higher-risk surface transportation assets (see figure 2). Given TSA’s definitions of higher-risk surface transportation assets, public transportation and passenger railroads and over-the-road bus operations are located in larger metropolitan areas. Freight railroad and pipeline companies with higher-risk assets have headquarters in a range of locations, including large metropolitan areas and smaller rural areas. Appendix I contains a complete list of the 62 geographic areas.

Figure 2: Locations with More Than One Higher-Risk Surface Transportation Asset, as Defined by the Transportation Security Administration in Fiscal Year 2023



Source: GAO analysis of Security Training for Surface Transportation Employees, 85 Fed. Reg. 16,456 (Mar. 23, 2020) and Transportation Security Administration information; GAO (illustrations). | GAO-24-106382

Surface Transportation Security Information Sharing Roles and Responsibilities

TSA and DHS I&A both coordinate intelligence and other information related to U.S. transportation security, but TSA is the lead agency for providing transportation security-related information to public and private transportation stakeholders.¹⁵

- TSA is the lead agency for providing transportation security-related information to other DHS components and state, local, tribal, and

¹⁵See 49 U.S.C. § 114(f).

private sector (SLTPS) entities, including surface transportation asset owners and operators.¹⁶

TSA's Office of Intelligence and Analysis—which is a separate office from DHS I&A—is responsible for sharing transportation security intelligence, conducting intelligence reporting on transportation security incidents, developing all-source intelligence, and vetting products that are shared with security and transportation industry professionals. TSA's intelligence staff include headquarters and field-based staff. For the purposes of this report, TSA field-based intelligence staff refers specifically to TSA Field Intelligence Officers. These staff share unclassified and classified intelligence products with internal and external transportation stakeholders through email distribution and briefings, among other tasks.

- DHS I&A is responsible for supporting DHS's mission of protecting Americans from terrorism and other homeland security threats by providing internal stakeholders with timely and actionable intelligence.¹⁷ Intelligence topics covered include threats to critical infrastructure, which could include surface transportation assets. DHS I&A is statutorily responsible for ensuring appropriate exchanges of information—including law enforcement information relating to threats of terrorism—with SLTPS entities.¹⁸ DHS I&A is also a member of the U.S. Intelligence Community, which consists of 18 executive branch

¹⁶Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*, designated DHS and the Department of Transportation as the two agencies responsible for overseeing the security and resilience of the transportation systems sector, which includes surface transportation. To address its transportation sector security responsibilities, DHS provides strategic security planning and guidance, promotes a national unity of effort using the whole-of-government approach, and coordinates the overall federal effort to promote the security and resilience of the nation's transportation assets, infrastructure, and systems. The Department of Transportation coordinates with its operating administrations, which directly manage the transportation programs that affect the security and resilience of critical transportation infrastructure to ensure a safe, efficient, and accessible transportation system. According to DHS, DHS delegated its responsibilities under Presidential Policy Directive 21 for surface transportation modes to TSA. DHS also delegated responsibility for aviation security to TSA; it delegated responsibility for maritime security to the U.S. Coast Guard.

¹⁷Consistent with the Homeland Security Act of 2002, DHS defines terrorism to mean any activity that involves an act that (i) is dangerous to human life or potentially destructive of critical infrastructure or key resources; and (ii) is a violation of the criminal laws of the United States or of any State or other subdivision of the United States; and appears to be intended (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping. Pub. L. No. 107-296, § 2(15), 116 Stat. 2135, 2141 (codified at 6 U.S.C. § 101(18)).

¹⁸See 6 U.S.C. §§ 121, 124h.

organizations that gather, analyze, and produce the intelligence necessary to conduct foreign relations and national security activities.¹⁹

DHS I&A's intelligence staff also includes headquarters and field-based staff in a variety of roles, including regional directors, human intelligence collection operations managers, intelligence officers, reports officers, and regional intelligence analysts.²⁰ For the purposes of this report, DHS I&A field-based intelligence staff refers specifically to intelligence officers. According to DHS I&A officials, intelligence officers are DHS I&A's primary liaisons in fusion centers and other field locations. These staff are responsible for collecting, analyzing, and disseminating threat information about topics that meet a national or departmental mission. Such staff are also responsible for providing unclassified and classified threat information to SLTPS entities. According to DHS I&A, they may do so via briefings or by facilitating access to DHS information sharing systems such as the unclassified Homeland Security Information Network or the classified Homeland Secure Data Network. These staff may also produce intelligence products or provide analytical support to fusion center products, among other tasks.

In addition to TSA and DHS I&A, several other entities play a role in information sharing, including fusion centers and surface transportation owners and operators.²¹

- Fusion centers are to serve as focal points to help improve the sharing of information among federal and SLTPS entities. Every state and many major urban areas own and operate fusion centers to collaborate and share resources, expertise, and information with the goal of maximizing the ability to gather and analyze information related to law enforcement, homeland security, public safety, and

¹⁹50 U.S.C. § 3003(4).

²⁰According to DHS I&A officials, regional directors are responsible for managing interagency relationships with government partners; human intelligence collection operations managers are responsible for managing the collection and review of raw information and intelligence from human sources; reports officers are responsible for identifying and reporting information that meets DHS requirements for reporting unevaluated or raw intelligence information to the intelligence community; and regional intelligence analysts are responsible for overseeing the analysis of the information collected in the region. Generally, these positions do not have direct relationships with surface transportation owners and operators.

²¹

terrorism.²² The composition of fusion center staff varies based on the fusion center's resources, area of operation, and focus. Federal entities that have deployed staff to fusion centers include DHS I&A, U.S. Customs and Border Protection, the Bureau of Alcohol, Tobacco, Firearms, and Explosives, and FBI, among others.

- Surface transportation owners and operators, both public and private, have principal responsibility for the safety and security of the people using their services.²³ Given the varied nature of services provided and the associated security risks of each entity, the specific roles and responsibilities also vary. Generally, owners and operators receive threat information and share it internally. Some owners and operators are also required to report incidents, potential threats, and significant security concerns to TSA and cybersecurity incidents to CISA.²⁴ Industry associations represent many owners and operators in collaborative forums with federal and SLTPS entities, such as federally authorized advisory committees.²⁵

Relevant TSA and DHS I&A Intelligence Products

TSA and DHS I&A field-based intelligence staff may share several types of intelligence and information products with surface transportation

²²See generally 6 U.S.C. § 124h(k)(1).

²³Depending on location and other factors, transportation owners and operators may be public, private, or a mixture of both. Public transportation owners and operators in this context refers to state, local, or tribal entities that operate regular, continuing shared-ride surface transportation services that are open to the general public or are open to a segment of the general public defined by age, disability, or low income. Private sector owners and operators refers to entities not owned by the government that operate surface transportation assets, such as freight rail companies or intercity bus operators.

²⁴Higher-risk surface transportation owners and operators are required to report all potential threats and significant security concerns involving transportation-related operations in the United States or transportation to, from, or within the United States as soon as possible and within 24 hours of discovery by the methods prescribed by TSA, among other things. See 49 C.F.R. § 1570.203 (directing each owner/operator identified in §§ 1580.1, 1582.1, and 1584.101 to report significant security concerns as provided). In addition, TSA security directives require some freight railroads, public transit and passenger railroads, and pipeline owners and operators to report cybersecurity incidents to CISA, among other requirements. See TSA, *Security Directives 1580-21-01B (freight railroad)* (Springfield, VA; Oct. 24, 2023); TSA, *1582-21-01B (public transportation and passenger rail)* (Springfield, VA; Oct. 24, 2023), and TSA, *Pipeline-2021-01C (pipeline)* (Springfield, VA; May 29, 2023).

²⁵Relevant industry associations include the Association of American Railroads, the American Public Transportation Association, the American Petroleum Institute, the American Gas Association, and the American Bus Association.

stakeholders.²⁶ Generally, these products fall into two categories: (1) finished intelligence products and (2) raw information reports or unfinished intelligence. In the context of this report, finished intelligence products refer to products—regardless of form or format—that reflect analytic assessments, judgment, or other analytic input of DHS I&A or TSA intelligence personnel (in headquarters or field locations). These products may be disseminated outside of DHS. Raw information reports, or unfinished intelligence, refer to products that contain unanalyzed content that is the same or substantially the same as when it was acquired.

DHS I&A and TSA may share classified and unclassified information with surface transportation stakeholders. Unclassified information may still be considered sensitive and contain other designations, such as For Official Use Only, Sensitive Security Information, and Law Enforcement Sensitive.²⁷ In addition, TSA and DHS I&A field-based intelligence staff may share information in other formats with stakeholders, such as briefings.

Below are examples of intelligence products that DHS I&A and TSA might share with surface transportation stakeholders (see table 1).

²⁶Throughout this report, we use “surface transportation stakeholders” to refer to the staff we interviewed from surface transportation owners and operators, surface transportation modal associations, and fusion centers.

²⁷Controlled Unclassified Information is information other than classified information that the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, which requires special handling and controls to prevent the unauthorized disclosure to the public or other individuals without an official need-to-know. See generally 32 C.F.R. § 2002.4(h). Sensitive Security information is any information obtained or developed in the conduct of security activities, including research and development, the disclosure of which TSA has determined would (1) constitute an unwarranted invasion of privacy (including, but not limited to, information contained in any personnel, medical, or similar file); (2) reveal trade secrets or privileged or confidential information obtained from any person; or (3) be detrimental to the security of transportation. 49 C.F.R. § 1520.5.

Table 1: Examples of Transportation Security Administration (TSA) and Department of Homeland Security Office of Intelligence and Analysis (DHS I&A) Intelligence and Information Products

Product	Description	Producing Organization	Classification
Regional Intelligence Notes	Finished intelligence products that look at threats impacting the homeland security environment, which could include critical infrastructure in a particular region. They contain analysis based on evidence and research gathered from technical open-source reports from multiple sources inside and outside of government. For example, one such report assessed trends and intelligence collection in the Gulf Coast region, including those targeting pipeline facilities.	DHS I&A	Unclassified or classified
Intelligence Information Reports	Raw information reports that provide details on various threats. They are shared with the Intelligence Community. For example, one such report described a cyberattack targeting a public transportation entity’s public-facing website.	TSA and DHS I&A	Unclassified or classified
Field Information Reports	Raw information reports that describe incidents including suspected domestic terrorist activities, insider threats, and cyber threats and vulnerabilities. They are shared with the DHS Intelligence Enterprise, which refers to DHS entities that support intelligence-related activities. For example, one such report described the discovery of suspicious items on a rail car.	TSA and DHS I&A	Unclassified
Quick Looks	Finished intelligence products that provide stakeholders with immediate insights and perspectives on emergent events.	TSA	Unclassified or classified
Intelligence Briefings	Provided to various public and private surface transportation stakeholders, periodically or as needed. These briefings occur at the headquarters or local level and may be conducted face-to-face, via secure web conference tools for unclassified information, or through secure teleconference and video teleconferences for classified information.	TSA and DHS I&A	Unclassified or classified

Source: GAO analysis of DHS and TSA information. | GAO-24-106382

Protection of Privacy, Civil Rights, and Civil Liberties

Various requirements govern the protection of personally identifiable information by federal agencies, including the use of U.S. persons’ information in intelligence and information products. For example, the Privacy Act of 1974, as amended, places limitations on agencies’ collection, disclosure, and use of personal information maintained in systems of records.²⁸ Agencies generally operationalize statutory requirements to protect privacy, civil rights, and civil liberties through agency-specific policies and procedures.

In addition, Intelligence Community elements that collect, retain, and disseminate information concerning U.S. persons—including DHS I&A—are required to establish procedures governing these activities.²⁹ DHS I&A issued its Intelligence Oversight Guidelines in 2017 to address this

²⁸5 U.S.C. § 552a(e).

²⁹Exec. Order No. 12333, 46 Fed. Reg. 59,941, 59,950 (Dec. 4, 1981).

requirement.³⁰ These guidelines identify various safeguards to help ensure that I&A personnel protect the privacy, civil rights, and civil liberties of U.S. persons when conducting intelligence activities. In addition, DHS I&A has issued other policies and procedures regarding how personnel are to protect privacy, civil rights, and civil liberties. For example, DHS I&A issued procedures establishing the review process for DHS I&A finished intelligence products, which were developed, in part, to protect privacy rights of U.S. persons and other individuals.

TSA and DHS I&A Used Different Approaches and Allocated Field-Based Intelligence Staff to Many Areas with Higher-Risk Surface Transportation Assets

TSA and DHS I&A differed in their consideration of surface transportation security risks when allocating field-based intelligence staff. Each allocated staff to approximately half of the 62 locations with higher-risk surface transportation assets and, according to agency officials, staff in other locations were assigned to all of the remaining areas with higher-risk surface transportation assets. When allocating field-based intelligence staff, TSA and DHS I&A took into account their mission priorities, which are broader than surface transportation security. Though their approaches differed, TSA allocated field-based intelligence staff to 30 of the 62 geographic areas with higher-risk surface transportation assets and DHS I&A allocated field-based intelligence staff to 29 of those 62 areas.³¹ According to TSA and DHS I&A officials, all the remaining locations with higher-risk surface transportation assets that did not have field-based intelligence staff located within the geographic area were supported by field-based intelligence staff in other locations.

TSA and DHS I&A Differed in Their Consideration of Surface Transportation Security Risks when Allocating Field-Based Intelligence Staff

TSA and DHS I&A took different approaches to considering surface transportation security risks when allocating field-based intelligence staff because they also took into account their other mission priorities. Section 6418(a) of the National Defense Authorization Act for Fiscal Year 2022 included a provision that DHS prioritize the assignment of TSA and DHS I&A intelligence staff to locations with higher-risk surface transportation assets.³² According to TSA and DHS I&A officials, their approaches to allocating field-based intelligence staff reflected their respective missions and priorities, which include or have a nexus to surface transportation security but are not limited to that issue. TSA's and DHS I&A's field-based

³⁰Department of Homeland Security, Office of Intelligence and Analysis, *Office of Intelligence and Analysis Intelligence Oversight Program and Guidelines*, Instruction IA-1000 (Washington, D.C.: Jan. 19, 2017).

³¹TSA and DHS I&A did not allocate field-based intelligence staff to the same areas with higher-risk surface transportation assets, though there was overlap.

³²§ 6418(a), 135 Stat. at 2415.

intelligence staff are responsible for supporting local intelligence needs on a wide range of topics. As previously noted, TSA field-based intelligence staff provide intelligence support to TSA operational components and transportation security stakeholders for all modes of transportation. DHS I&A field-based intelligence staff deliver intelligence to SLTPS partners on a range of issues, including counterterrorism, transnational organized crime, cyber threats, counterintelligence and foreign malign influence, and economic security.

TSA considered the location of certain higher-risk surface transportation assets in its allocation of field-based intelligence staff.³³ According to TSA officials, in fiscal year 2016, TSA received authorization to increase its field intelligence program, from 61 positions to 87 positions.³⁴ To inform where it should allocate those new staff, TSA developed a tool in fiscal year 2017 that used a weighted scoring method to account for the relative importance of various aviation and surface transportation risk factors. Surface transportation-related factors—specifically, the size of the area’s public transportation system and the presence of select higher-risk freight railroad, trucking, or pipeline company headquarters—accounted for 20 percent of the weighting TSA used to prioritize where to allocate field-based intelligence staff.³⁵

Further, according to TSA officials, TSA considered the location of the headquarters of certain asset types whose systems span multiple states or regions because the company’s security staff with whom field-based intelligence staff generally coordinate are often headquarters-based. TSA officials said the tool was most valuable in identifying smaller airports where TSA should allocate field-based intelligence staff because of surface transportation factors. For example, TSA allocated an intelligence

³³TSA field-based intelligence staff are assigned to airports but are intended to be the intelligence advisor to TSA field leadership on threats and intelligence for all transportation modes in the geographic area for which they are responsible.

³⁴According to TSA officials, TSA is authorized to hire up to 87 positions for its field intelligence program; as of fiscal year 2023, TSA budgeted for 75 of those. According to TSA officials, this includes 67 field-based intelligence staff, 4 regional managers, and 4 operations officers. According to TSA officials, as budgets permit, it plans to hire additional field-based intelligence staff. Based on its assessment of its staff allocation, TSA plans to place those additional staff in airports where there is already a field-based intelligence presence.

³⁵Other factors included airport-specific factors, such as annual passenger throughput and the number of known or suspected terrorists that pass through the airport each year, as well as other measures of risk, such as a cross-modal measure of transportation modes and their terrorism target attractiveness scores.

staff position to Omaha, Nebraska, because a higher-risk freight rail company is headquartered there.

According to TSA officials, updating the model and its data is costly, as is redeploying staff. Given those costs, because the surface transportation assets TSA considered higher-risk have not generally changed over time and the authorized number of field-based intelligence staff has not changed since fiscal year 2016, TSA officials determined it did not need to regularly reassess its allocation of staff positions. Moreover, according to TSA officials, the wide geographical dispersion of field-based intelligence staff across the country enabled the agency to provide intelligence support to asset owners and operators whose systems or operations span multiple states or regions.

DHS I&A did not explicitly consider the location of higher-risk surface transportation assets in allocating field-based intelligence staff because it prioritized allocating field-based intelligence staff to each of the nation's primary and recognized fusion centers. According to DHS I&A, the creation of its field-based intelligence staff program is linked by statute to support for fusion centers as the hub for state and regional information sharing.³⁶ Specifically, that statute calls on DHS I&A, among other federal entities, to assign intelligence staff to fusion centers to support SLTPS entities. According to DHS I&A, its first priority was to allocate at least one field-based intelligence staff to each of the 80 primary and recognized fusion centers, which, as of fiscal year 2023, it had done. As noted above, DHS I&A intelligence staff are responsible for all threats, including terrorism, transnational organized crime, cyber threats, and economic security. Given those broad responsibilities, according to DHS I&A officials, the location of a higher-risk surface transportation asset was not a factor in allocating intelligence staff.

According to one senior DHS I&A official, now that it has reached its initial goal of allocating field-based intelligence staff to each fusion center, DHS I&A may consider the location of higher-risk surface transportation assets if its intelligence staff were to increase. Further, as discussed later in this report, although the presence of higher-risk surface transportation assets was not a factor in DHS I&A's staff allocation, according to DHS I&A officials, all of the areas with higher-risk surface transportation assets

³⁶See generally 6 U.S.C. § 124(h).

were supported by DHS I&A field-based intelligence staff who were either located in the geographic area of the asset or within the same state.

TSA and DHS I&A Allocated Field-Based Intelligence Staff Nationwide, Including Many Areas with Higher-Risk Surface Transportation Assets

Though TSA and DHS I&A differed in their consideration of surface transportation security risks when allocating field-based intelligence staff, each allocated staff to approximately half of the 62 locations with higher-risk surface transportation assets, and staff in other locations were assigned to support the remaining areas. TSA allocated field-based intelligence staff to 30 of the 62 geographic areas with higher-risk surface transportation assets and DHS I&A allocated field-based intelligence staff to 29 of those 62 areas.³⁷ As of the end of fiscal year 2023, field-based intelligence staff were on-board in most of the geographic locations with higher-risk assets with allocated positions.³⁸ According to TSA and DHS I&A, the remaining locations with higher-risk surface transportation assets that did not have field-based intelligence staff located within the geographic area were supported by field-based intelligence staff in other locations.

TSA field-based intelligence staff. TSA field-based intelligence staff are located at airports and are to provide intelligence support to TSA entities and external stakeholders for all modes of transportation, including surface transportation. In fiscal year 2023, TSA allocated a total of 67 field-based intelligence staff assigned to 64 airports across the country. The location of these field-based intelligence staff included geographic

³⁷For the purposes of this report, field-based intelligence staff were determined to be in the same geographic area as the higher-risk surface transportation asset if the airport or fusion center to which staff were allocated was within the same geographic area as the assets or operations described in 49 C.F.R. §§ 1580.101, 1582.101, and 1584.101. For higher-risk surface transportation assets in locations other than those described in the cited regulations, field-based intelligence staff were determined to be in the same geographic area if the airport or fusion center to which the staff were allocated were within an approximately 10-mile buffer area around the city where the asset was located. We used the 10-mile buffer area to correspond with the 10-mile buffer area applied to high threat urban areas in federal regulations. 49 C.F.R. § 1580.101, App. A (noting that “a 10-mile buffer extending from the border of the combined area” is included in the geographic areas for all High Threat Urban Areas). TSA and DHS I&A did not allocate field-based intelligence staff to the same areas with higher-risk surface transportation assets, though there was overlap.

³⁸For the purposes of this report, “allocated” refers to staff positions for which TSA or DHS I&A have approved funding and assigned to a location. “On-board” refers to positions to which TSA or DHS I&A have hired staff; otherwise, the position is considered “vacant.”

areas with and without higher-risk surface transportation assets.³⁹ Some geographic areas have more than one airport with assigned field-based intelligence staff, and some airports were assigned more than one field-based intelligence staff person.⁴⁰

In fiscal year 2023, TSA allocated at least one field-based intelligence staff person to 30 of the 62 locations with higher-risk surface transportation assets (see table 2). Across these locations, TSA allocated a total of 42 field-based intelligence staff positions, of which three positions were vacant as of the end of fiscal year 2023. As a result of the vacancies, TSA field-based intelligence staff were on-board in 27 of the 30 locations with higher-risk surface transportation assets where TSA had allocated staff positions.⁴¹ See Appendix I for more information about the locations and status of allocated staff.

According to TSA officials, field-based intelligence staff assigned to other airports in the region are to support stakeholders—including surface transportation owners and operators—in locations where the field-based intelligence staff position is vacant. For example, the field-based intelligence staff in Portland, Maine, was assigned to support stakeholders in the Boston area until TSA filled the position. Similarly, according to TSA, the 32 locations with higher-risk surface transportation assets that did not have TSA field-based intelligence staff located within the geographic area were supported by field-based intelligence staff in other locations. For example, the field-based intelligence staff located in El Paso, Texas, was responsible for supporting and sharing information with stakeholders associated with the higher-risk surface transportation

³⁹Three field-based intelligence staff were assigned to provide support to multiple airports. For the purposes of quantifying the number of airports where TSA assigned field-based intelligence staff, we counted the airport where they were officially stationed. In addition to field-based intelligence staff, TSA had four operations officers who were assigned to airports. In fiscal year 2023, operations officers also executed field-based intelligence staff responsibilities for a portion of their time. For the purposes of quantifying the number of field-based intelligence staff, we only counted the staff executing those duties full-time.

⁴⁰For example, TSA allocated field-based intelligence staff to San Francisco International Airport, Oakland International Airport, and San Jose Mineta International Airport, which are all in the San Francisco Bay Area. As another example, two field-based intelligence staff were assigned to Washington-Dulles International Airport in the Greater Washington D.C./National Capital region.

⁴¹As of the end of fiscal year 2023, there were three vacant TSA field-based intelligence staff positions in locations with higher-risk surface transportation assets where TSA had allocated staff positions. All three vacancies were at airports in locations where no other TSA field-based intelligence staff were allocated—Boston area, New Orleans area, and San Diego area.

assets in Albuquerque, New Mexico, because there was no TSA field-based intelligence staff presence there. Appendix I includes TSA staffing information by location and type of higher-risk surface transportation asset.

Table 2: Transportation Security Administration (TSA) Field-Based Intelligence Staff Allocation by Location Type for Fiscal Year 2023^a

Location type	Number of locations with at least one TSA field-based staff allocated ^b	Number of TSA field-based staff on-board at higher-risk locations ^c
All locations with higher-risk surface transportation assets	30 of 62 locations	39 of 42 allocated positions
Locations with higher-risk public transportation and passenger railroads	8 of 8 locations	17 of 18 allocated positions
Locations with higher-risk over-the-road bus operations	10 of 10 locations	19 of 21 allocated positions
Locations with headquarters of higher-risk freight railroad companies	14 of 24 locations	19 of 20 allocated positions
Locations with headquarters of higher-risk pipeline companies	29 of 52 locations	38 of 41 allocated positions

Source: GAO analysis of TSA information and data. | GAO-24-106382

^aLocation and staff allocation numbers for individual higher-risk surface transportation asset types do not sum because some locations have more than one type of higher-risk surface transportation asset present.

^b“Allocated” refers to staff positions for which TSA has approved funding and assigned to a location.

^c“On-board” refers to positions to which TSA has hired staff; otherwise, the position is considered “vacant.”

DHS I&A field-based intelligence staff. DHS I&A generally assigned field-based intelligence staff to one of the nation’s 80 fusion centers, where they provide intelligence support to SLTPS stakeholders and decisionmakers at all levels.⁴² In fiscal year 2023, DHS I&A allocated 82 field-based intelligence staff to 82 locations both with and without higher-

⁴²Two field-based intelligence staff are assigned locations in New York City where there is no fusion center. State governors designate fusion centers, which are owned and operated by state and local entities. New York has designated a primary fusion center located in its capital, Albany; it does not have any regional fusion centers. According to field-based intelligence staff, New York City’s High Intensity Drug Trafficking Center serves a similar purpose as a fusion center and brings together federal, state, and local law enforcement entities in the area.

risk surface transportation assets.⁴³ Fusion centers are designated by the state governor and owned and operated by state and local entities. Each state designates a primary fusion center that typically provides information sharing and analysis for the entire state. Many states also have recognized fusion centers that typically provide information sharing and analysis for a major urban area.

In fiscal year 2023, DHS allocated at least one field-based intelligence staff to 29 of the 62 locations with higher-risk surface transportation assets (see table 3). Across these locations, DHS I&A allocated a total of 36 field-based intelligence staff positions, of which four were vacant as of the end of fiscal year 2023. As a result of the vacancies, DHS I&A field-based intelligence staff were on-board in 27 of the 29 locations with higher-risk surface transportation assets where DHS I&A had allocated staff positions.⁴⁴ See Appendix I for more information about the locations and status of allocated staff.

Given the responsibilities of primary fusion centers, which are to provide intelligence support for the entire state, the 33 geographic areas with higher-risk surface transportation assets that did not have DHS I&A field-based intelligence staff located within the geographic area at a recognized major urban area fusion center were supported by staff located at the statewide primary fusion center. For example, according to DHS I&A officials, the field-based intelligence staff located at the fusion center in Nashville, Tennessee, was responsible for supporting and sharing information, in collaboration with TSA, with stakeholders associated with the higher-risk surface transportation assets in Memphis, Tennessee, because there was no DHS I&A field-based intelligence staff

⁴³DHS I&A had 37 other staff assigned to fusion centers, including human intelligence collection operations managers, reports officers, and regional intelligence analysts. For the purposes of this report, we focus on intelligence officers, which we refer to throughout as "field-based intelligence staff," because they are DHS I&A's primary liaisons in the field for information sharing. In addition to the 80 fusion centers, DHS I&A also assigned field-based intelligence staff to two non-fusion center locations in New York City.

⁴⁴As of the end of fiscal year 2023, there were four vacant DHS I&A field-based intelligence staff positions in locations with higher-risk surface transportation assets where DHS had allocated staff positions. Two vacancies were at fusion centers in locations where other field-based intelligence staff were allocated and on-board—Dallas-Ft. Worth area, and Philadelphia-Southern New Jersey area. Two vacancies were at fusion centers in locations where no other DHS I&A field-based intelligence staff were allocated—Bismarck, ND and Salt Lake City area.

presence there. Appendix I includes DHS I&A staffing information by location and type of higher-risk surface transportation asset.

Table 3: Department of Homeland Security (DHS) Office of Intelligence and Analysis (I&A) Field-Based Intelligence Staff Allocation by Location Type for Fiscal Year 2023^a

Location type	Number of locations with at least one DHS I&A field-based staff allocated ^b	Number of DHS I&A field-based staff on-board at higher-risk locations ^c
All locations with higher-risk surface transportation assets ^c	29 of 62 locations	32 of 36 allocated positions
Locations with higher-risk public transportation and passenger railroads	8 of 8 locations	12 of 13 allocated positions
Locations with higher-risk over-the-road bus operations	10 of 10 locations	15 of 17 allocated positions
Locations with headquarters of higher-risk freight railroad companies	13 of 24 locations	15 of 17 allocated positions
Locations with headquarters of higher-risk pipeline companies	27 of 52 locations	30 of 34 allocated positions

Source: GAO analysis of DHS I&A and Transportation Security Administration information and data. | GAO-24-106382

^aLocation and staff allocation numbers for individual higher-risk surface transportation asset types do not sum because some locations have more than one type of higher-risk surface transportation asset present.

^b“Allocated” refers to staff positions for which DHS I&A has approved funding and assigned to a location.

^c“On-board” refers to positions to which DHS I&A has hired staff; otherwise, the position is considered “vacant.”

Field-Based Intelligence Staff and Other Public and Private Entities Participate in Information Sharing Activities Related to Surface Transportation Security

Field-based Intelligence Staff Played a Small Role in Generating Information Products about Surface Transportation and Primarily Disseminated Information to Local Stakeholders

TSA and DHS I&A field-based intelligence staff played a small role in generating information products about surface transportation security. Specifically, TSA field-based intelligence staff did not have a role in generating finished intelligence products, though some generated other types of information products. DHS I&A field-based intelligence staff generated intelligence products, but none were related to surface transportation. However, many field-based intelligence staff played an active role in disseminating information from a range of sources to surface transportation stakeholders. TSA and DHS I&A field-based intelligence staff disseminated information primarily via email and oral briefings.

Role in Generating Surface Transportation Security Products

TSA and DHS I&A field-based intelligence staff played a small role in generating products about surface transportation security.

TSA. TSA field-based intelligence staff did not have a role in generating finished intelligence products, though some generated other types of information products about surface transportation security. According to TSA, generating finished intelligence products is primarily the responsibility of headquarters-based intelligence staff.

From fiscal year 2018 through fiscal year 2023, TSA headquarters-based intelligence staff generated between 17 and 62 finished intelligence

products related to surface transportation per year.⁴⁵ Some of these products were annual reports, such as security threat assessments TSA generated for each transportation mode. The remainder were event-driven products. For example, in fiscal year 2019 when TSA generated 62 finished intelligence products, 29 of those products were travel briefings published for TSA's Law Enforcement Federal Air Marshal Service. These briefings focused on threats to surface transportation for force protection purposes. Field-based intelligence staff may provide examples or other information to headquarters-based staff, but they do not have a role in drafting these products.

While TSA's field-based intelligence staff did not generate finished intelligence products, these staff did generate raw information reports about transportation security incidents—including surface transportation security incidents.⁴⁶ From fiscal year 2020 through fiscal year 2023, TSA reported that its field-based intelligence staff generated between 51 and 143 raw information reports, known as field information reports, per year about surface transportation-related incidents.⁴⁷ These reports capture a variety of incident types, including tampering, trespassing, vandalism, cyber incidents, and suspicious activity.⁴⁸ TSA field-based intelligence staff generate these reports in a system available to certain intelligence and law-enforcement staff across DHS and its component agencies, but these products generally were not available to surface transportation owners and operators.

Some TSA field-based intelligence staff we interviewed also said they generated briefings based on finished intelligence products or information they received from other sources. TSA field-based intelligence staff also delivered periodic and ad hoc briefings to surface transportation owners, operators, and other stakeholders. For example, one TSA field-based intelligence staff person we interviewed described delivering briefings to

⁴⁵In the context of this report, finished intelligence refers to products—regardless of form or format—that reflect analytic assessments, judgment, or other analytic input of TSA or DHS I&A intelligence personnel (in headquarters or field locations).

⁴⁶Raw information reports or unfinished intelligence refer to products that contain unanalyzed content that is the same or substantially the same as when it was acquired.

⁴⁷In comparison, over the same period, field-based intelligence staff generated between 962 and 1,322 field information reports about aviation-related incidents. Fiscal year 2020 was the first full year of data about field information reports TSA tracked and analyzed.

⁴⁸Suspicious activity refers to observed behavior that may indicate pre-operational planning associated with terrorism or terrorism-related crime.

share information about the annual security threat assessments TSA generated for each transportation mode. According to field-based intelligence staff we interviewed, they developed those briefings using materials prepared by TSA headquarters-based staff and other sources available to them, including DHS I&A and the Cybersecurity and Infrastructure Security Agency (CISA).

DHS I&A. DHS I&A field-based intelligence staff generated intelligence products, but none were related to surface transportation specifically. According to DHS I&A, from fiscal year 2018 through fiscal year 2023, its field-based intelligence staff generated between 13 and 57 finished intelligence products per year. In addition, DHS I&A field-based intelligence staff contributed to between 10 and 33 fusion center-generated products per year by drafting short sections included in those reports. These staff also generated between 18 and 164 regional perspectives each year that provided regional context to finished intelligence products generated by DHS and other agencies. According to DHS I&A, although none of these products were specifically related to surface transportation security threats, they may nonetheless be relevant and useful for the situational awareness of surface transportation owners and operators.

According to DHS I&A, it defers to TSA on generating products specifically related to transportation security. DHS I&A officials said that DHS I&A field-based intelligence staff would refer information about surface transportation security threats to TSA counterparts in addition to sharing with appropriate federal and state, local, tribal, and private sector (SLTPS) entities.

Role in Disseminating Surface Transportation Products

While field-based intelligence staff played a limited role in generating products about surface transportation, they played an active role in disseminating information from a range of sources to surface transportation stakeholders. TSA field-based intelligence staff received information about surface transportation security threats from headquarters-based intelligence staff, as well as various federal entities, including CISA and FBI. They also received relevant information from SLTPS sources. According to TSA, TSA field-based intelligence staff reviewed the information and disseminated it as often as needed based on the content of the information and its relevance to the stakeholders in their area of responsibility. DHS I&A field-based intelligence staff may receive information relevant to surface transportation stakeholders from one of its analytical entities, each of which focuses on a topical area (e.g.,

counterterrorism or cybersecurity) and produce intelligence products.⁴⁹ According to DHS I&A officials, DHS I&A field-based intelligence staff may also share information prepared in anticipation of special events, such as the Macy's Thanksgiving Day Parade in New York City, which can include surface transportation-related security concerns.

Most TSA and DHS I&A field-based intelligence staff disseminated information via email. Two-thirds (10 of 15) of the field-based intelligence staff we interviewed said they shared information with surface transportation stakeholders via email distribution lists they maintain. Some field-based intelligence staff also shared information via intelligence briefings. Field-based intelligence staff did not post information to the Homeland Security Information Network, but some said they might direct surface transportation stakeholders to products shared on that platform.⁵⁰

Many Public and Private Entities Disseminated Information about Surface Transportation Security

In addition to TSA and DHS I&A field-based intelligence staff, surface transportation stakeholders we interviewed said they received relevant security information from several other sources. These sources included staff from other TSA offices, as well as federal and non-federal entities.

TSA Office of Policy, Plans, and Engagement. Staff were the primary points of contact for sharing unclassified transportation security information with owners, operators, and other stakeholders. These staff include, for example, industry engagement managers who are assigned to cover a mode of transportation and serve as liaisons to respective owners, operators, and other stakeholders.

TSA Surface Operations staff. Staff, such as surface inspectors, shared information with surface transportation owners and operators. Surface Operations staff provide regulatory and structured oversight of surface transportation systems. Those staff support information sharing by delivering trainings and information products intended to assist surface transportation stakeholders with identifying, preventing, responding to, and recovering from a terrorist attack. In some locations, surface

⁴⁹As of the end of fiscal year 2023, DHS I&A's topical entities were the Counterterrorism Center, the Cyber Intelligence Center, the Nation State Threat Center, and the Transborder Security Center.

⁵⁰The Homeland Security Information Network is a web-based platform operated by DHS to facilitate sensitive but unclassified information sharing and collaboration among federal and SLTPS entities.

inspectors distributed information directly to surface transportation stakeholders via email at the request of local field-based intelligence staff.

TSA Surface Information Sharing Cell. This initiative brought together government and private sector personnel to facilitate surface transportation-related threat and security information sharing and collaboration. The Surface Information Sharing Cell is an initiative managed by TSA staff in its Threat Intelligence Sharing Branch. These staff hosted biweekly conference calls to share finished intelligence products from TSA and other agencies, as well as open-source reporting, with surface transportation owners, operators, and other stakeholders. They also hosted quarterly, in-person sessions for surface transportation stakeholders that included classified briefings delivered by TSA and DHS I&A intelligence staff. After an initial pilot phase, during which participation consisted of approximately 40 stakeholders, the Surface Information Sharing Cell's charter was approved in October 2022, and TSA officials considered it fully operational as of May 2023. As of October 2023, TSA estimated 277 stakeholders were members of the initiative.

Other federal information sources. Other federal entities disseminated information to surface transportation stakeholders about security topics relevant to their respective missions. Surface transportation stakeholders we interviewed reported receiving information from CISA, including automated alerts and information from field-based security advisors. Stakeholders we interviewed also said they received information from FBI's Joint Terrorism Task Forces in their geographic areas. Some stakeholders, including larger mass transit operators, had staff detailed to a Joint Terrorism Task Force, which facilitated information sharing. In addition, pipeline stakeholders said that the Department of Energy was a source of relevant security information.

Non-federal information sources. Non-federal entities also disseminated information to various sub-groups of surface transportation stakeholders. For example, some surface transportation stakeholders reported receiving security information relevant to the geographic area from local fusion centers. They also received information relevant to their transportation mode from industry associations. Information Sharing and Analysis Centers are also a source of information for surface

transportation stakeholders.⁵¹ For example, the Association of American Railroads manages a system that disseminates advisories and information briefs on potential terrorist tactics, malicious cyber activity, rail-related threats and incidents, and other suspicious activity to its members.⁵² Information Sharing and Analysis Centers comprised of sector-specific infrastructure owners and operators also collect, analyze, and disseminate actionable threat information to their members. Relevant Information Sharing and Analysis Centers include Downstream Natural Gas; Multi-State; Oil and Natural Gas; and Surface Transportation, Public Transportation, and Over-the-Road Bus.

Select Surface
Transportation
Stakeholders Said
Information Sharing
Processes Generally Met
their Needs

TSA, DHS I&A, and other entities shared information for awareness, which most surface transportation stakeholders we interviewed said generally met their needs. TSA and DHS I&A field-based intelligence staff we interviewed said that specific threats of terrorism involving a surface transportation asset have not been common since fiscal year 2018. However, according to TSA, field-based intelligence staff regularly monitored threats to surface transportation assets, including cyber actors. According to the 2023 Biennial National Strategy for Transportation Security, prepared by TSA, while surface transportation assets remained potential targets of malicious actors—including international and domestic terrorists—the aviation sector was the preferred target for terrorists seeking to conduct spectacular mass-casualty attacks.⁵³ Among the 15 field-based intelligence staff we interviewed, almost all (14 of 15) said terrorist threats to surface transportation assets in their respective areas

⁵¹Critical infrastructure owners and operators started creating Information Sharing and Analysis Centers in 1999 in response to *Presidential Decision Directive/NSC-63*, which strongly encouraged the creation of private-sector entities that could gather, analyze, appropriately sanitize, and share intelligence and information related to critical infrastructure. White House, *Presidential Decision Directive/NSC-63* (Washington, D.C.: May 22, 1998). DHS's *National Infrastructure Protection Plan* described Information Sharing and Analysis Centers as operational entities for coordinating federal agency and critical infrastructure owner and operator efforts, including information sharing. DHS, *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* (Washington, D.C.: 2013). Though some Information Sharing and Analysis Centers receive government funding, many require a paid membership for services.

⁵²The Association of American Railroads focuses on the safety and productivity of the U.S. freight rail industry. Its membership includes the major freight railroads in the United States, Canada, and Mexico, as well as Amtrak.

⁵³DHS, *Biennial National Strategy for Transportation Security*, April 18, 2023.

Example of a physical terrorist attack on a surface transportation asset

In April 2022, an individual set off a smoke-emitting device in a New York City subway car before shooting 10 people. The defendant pleaded guilty to 10 counts of committing a terrorist attack or other violence against a mass transportation vehicle and one count of discharging a firearm in furtherance of his attack.



Source: Department of Justice
IIIKWPHOTOIII25/stock.adobe.com. |
GAO-24-106382

were relatively uncommon. One incident that did take place since fiscal year 2018 occurred in the New York City subway (see sidebar).

Almost all of the surface transportation owners and operators we interviewed said threats relevant to their assets were not common or that security incidents were generally criminal in nature, rather than related to terrorism or targeted violence. Specifically, among the 15 surface transportation owners and operators we interviewed, 14 described threats relevant to their assets as not common or generally criminal in nature.⁵⁴

Though specific threats were not common, surface transportation stakeholders received general threat information and analytical products from the sources described above at varying frequencies. According to interviews with field-based intelligence staff and surface transportation stakeholders, field-based intelligence staff shared information as frequently as necessary, depending on security incidents in their area of responsibility and intelligence information they received. Some stakeholders we interviewed estimated they received information as frequently as once a week, while others said they received information approximately once a month or a few times a year.

In general, most surface transportation owners, operators, and other stakeholders we interviewed said the surface transportation security information they received from TSA, DHS I&A, and other sources met their needs and improved their situational awareness of security threats. Among the 15 surface transportation owners and operators we interviewed, 13 had positive assessments of information sharing about security threats.⁵⁵ According to surface transportation owners and operators we interviewed, the information they received—including summaries of recent security incidents—improved situational awareness. Many of the owners and operators with positive assessments described the information they received as timely, relevant, and of good quality.

Similarly, staff we interviewed from all six of the selected fusion centers had positive assessments of information sharing activities. Staff from four of the fusion centers said they did not observe negative impacts on information sharing because TSA field-based intelligence staff were assigned to an airport and not co-located at the fusion center. Staff from

⁵⁴One entity we interviewed did not address the topic.

⁵⁵The two remaining owners and operators raised issues with the timeliness and relevancy of the information they received. Both topics are described further below.

one fusion center said that while their relationship with local field-based intelligence staff was strong, they could see benefits of having the individual work from the fusion center. Staff from the remaining selected fusion center did not provide a perspective on the effect, if any, of co-location of TSA field-based intelligence staff on information sharing.

More than two-thirds of the surface transportation owners and operators we interviewed said they received the same information from multiple sources, but they generally preferred duplicative receipt over an alternative that may result in the information not being disseminated. Specifically, 11 of the 15 owners and operators we interviewed said they received the same or similar security-related information from multiple sources. However, these owners and operators also said that the duplication was not an issue, and most of them said it demonstrated that information was being shared among relevant parties or served as validation of areas to focus their attention.

Some surface transportation owners and operators, as well as representatives from industry organizations we interviewed, identified areas where information sharing could be improved. Specifically, representatives from one of the five industry groups we interviewed said products about security incidents would be more useful if they included additional analysis of trends. Representatives from another group said products would be more useful if they included information on how to mitigate the threat. Representatives from two industry organizations, as well as one of the owners and operators we interviewed, said that information sharing could be more timely, which would make it more actionable. However, other stakeholders considered the information useful and timely, and as previously noted, most surface transportation stakeholders we interviewed said generally met their needs.

Two-thirds of the surface transportation owners and operators we interviewed (10 of 15) told us that they rarely, if ever, provided feedback to TSA or DHS I&A about information sharing, and those that did said it was typically a request for additional information. If they did have feedback to share, many surface transportation stakeholders we interviewed said they would provide that information to TSA and DHS I&A via informal mechanisms, though they also have the opportunity to complete surveys about intelligence products and their information needs. Many surface transportation owners and operators we interviewed (6 of 15) said they would provide informal feedback on information products and their information needs to the TSA and DHS I&A field-based intelligence staff in their geographic area or their respective transportation

TSA and DHS I&A Have Measures Intended to Protect Privacy, Civil Rights, and Civil Liberties When Sharing Information about Surface Transportation Security

mode's TSA industry engagement manager. Stakeholders also had the opportunity to provide formal feedback. For example, there is a feedback survey at the end of finished intelligence products, including products by both TSA and DHS I&A. TSA also conducts an annual customer survey that includes some surface transportation stakeholders.⁵⁶

TSA and DHS I&A each have applicable policies that describe measures to protect privacy, civil rights, and civil liberties of U.S. persons in the context of information sharing, including sharing information about surface transportation security threats.⁵⁷ Those policies direct staff to retain information about U.S. persons for only as long as is necessary to fulfill its purpose. The policies also state that staff may not collect and retain information based solely on certain characteristics, including race, ethnicity, national origin, and religious affiliation, or for the sole purpose of monitoring activities protected by the First Amendment.⁵⁸

TSA measures to protect privacy, civil rights, and civil liberties.

TSA's activities are guided by DHS's *Federal Information Sharing Environment Privacy and Civil Liberties Protection Policy*, which applies

⁵⁶According to TSA officials, the response rate for surface transportation stakeholders in the fiscal year 2022 annual customer survey was approximately 15 percent and were not analyzed separately from other stakeholders.

⁵⁷For example, Department of Homeland Security, *Federal Information Sharing Environment Privacy and Civil Liberties Protection Policy*, Policy Directive 262-15 (Washington, D.C.: Jun. 5, 2009) and Department of Homeland Security, Office of Intelligence and Analysis, *Intelligence Oversight Program and Guidelines*, Instruction IA-1000 (Washington, D.C.: Jan. 19, 2017).

⁵⁸DHS I&A's Intelligence Oversight Guidelines include additional characteristics that staff may not use as the sole basis for intelligence activities. These are: gender, sexual orientation, gender identity, country of birth, or nationality. TSA is not subject to DHS I&A's guidelines; however, according to TSA officials, it does not use these characteristics as the sole basis for engaging in intelligence activities as a matter of practice.

to all DHS component agencies.⁵⁹ In keeping with that policy, TSA requires oversight of intelligence production to ensure appropriate protections for privacy, civil rights, and civil liberties consistent with relevant laws, such as the Privacy Act, and other DHS guidance. According to the policy, it is based on the Fair Information Practice Principles, which are central to the framework of the Privacy Act itself (see table 4).⁶⁰ For example, according to the policy, when sharing information that would identify a specific U.S. person, TSA is to minimize dissemination to what is necessary to address the needs of federal and non-federal stakeholders who are involved in efforts to identify, detect, and deter terrorism-related activities.

Table 4: Summary of Fair Information Practice Principles

Principle	Description
Collection limitation	The collection of personal information should be limited, obtained by lawful and fair means, and, where appropriate, with the knowledge or consent of the individual.
Data quality	Personal information should be relevant to the purpose for which it is collected, and should be accurate, complete, and current as needed for that purpose.
Purpose specification	The purposes for the collection of personal information should be disclosed before collection and upon any change to those purposes, and the use of the information should be limited to those purposes and compatible purposes.

DHS I&A's Intelligence Oversight Guidelines also state that staff may not engage in intelligence activities for the purpose of affecting the political process in the United States, to retaliate against a whistleblower, or to suppress or burden criticism or dissent. The department-wide DHS policy, which is applicable to TSA, does not have a parallel provision related to these aspects. Additionally, the First Amendment to the U.S. Constitution protects the freedoms of speech, press, and peaceful assembly, among others. U.S. Const. amend. I. The Privacy Act of 1974, as amended, restricts the ability of agencies that maintain a system of records to maintain records describing how any individual exercises First Amendment rights unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity. 5 U.S.C. § 552a(e)(7).

⁵⁹Department of Homeland Security, *Federal Information Sharing Environment Privacy and Civil Liberties Protection Policy*, Policy Directive 262-15 (Washington, D.C.: June 5, 2009).

⁶⁰The Fair Information Practice Principles are internationally recognized voluntary principles that were first proposed for protecting the privacy and security of personal information in the United States in 1973 by a U.S. government advisory committee. This advisory committee recommended enactment of a federal "Code of Fair Information Practice" applicable to automated personal data systems. In 1980, the Organisation for Economic Co-Operation and Development, an organization of 37 member countries, including the United States, developed a revised version that was widely adopted. In 2013, the Organisation for Economic Co-Operation and Development developed a revised version of the principles.

Principle	Description
Use limitation	Personal information should not be disclosed or otherwise used for purposes other than a specified purpose without consent of the individual or legal authority.
Security safeguards	Personal information should be protected with reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification, or disclosure.
Openness	The public should be informed about privacy policies and practices, and individuals should have ready means of learning about the use of personal information.
Individual participation	Individuals should have the following rights: to know about the collection of personal information, to access that information, to request correction, and to challenge the denial of those rights.
Accountability	Individuals controlling the collection or use of personal information should be accountable for taking steps to ensure the implementation of these principles.

Source: Organisation for Economic Co-Operation and Development. | GAO-24-106382

Note: The Fair Information Practice Principles are internationally recognized voluntary principles that were first proposed for protecting the privacy and security of personal information in the United States in 1973 by a U.S. government advisory committee. This advisory committee recommended enactment of a federal "Code of Fair Information Practice" applicable to automated personal data systems. In 1980, the Organisation for Economic Co-Operation and Development, an organization of 37 member countries, including the United States, developed a revised version that was widely adopted. In 2013, the Organisation for Economic Co-Operation and Development developed a revised version of the principles.

DHS I&A measures to protect privacy, civil rights, and civil liberties. In addition to DHS's *Federal Information Sharing Environment Privacy and Civil Liberties Protection Policy*, which applies to all DHS component agencies, as a member of the U.S. Intelligence Community, DHS I&A was required to develop guidelines governing the collection, retention, and dissemination of information concerning U.S. persons.⁶¹ In response to that requirement, DHS I&A issued its Intelligence Oversight Guidelines, which DHS I&A said is its primary guidance regarding privacy, civil rights, and civil liberties safeguards. According to one DHS I&A official, the guidelines are intended to distill and present constitutional, statutory, and policy protections in one document. DHS I&A issued its Intelligence Oversight Guidelines in 2017, following approval by the Attorney General. According to the guidelines, its requirements and restrictions are intended

⁶¹See Exec. Order No. 12333, 46 Fed. Reg. 59,941, 59,950 (Dec. 4, 1981), as amended. Executive Order 12333 provides that elements of the Intelligence Community are authorized to collect, retain, or disseminate information concerning U.S. persons only in accordance with procedures established by the head of the Intelligence Community element concerned or by the head of a department containing such element and approved by the Attorney General, consistent with the priorities provided in the Executive Order, after consultation with the Director. A U.S. person is: (1) a U.S. citizen, (2) a foreign national known by the intelligence element to be a lawful permanent resident, (3) an unincorporated association substantially composed of U.S. citizens or permanent residents, or (4) a corporation incorporated in the U.S., except for a corporation directed and controlled by a foreign government or governments. See also Department of Homeland Security, *Office of Intelligence and Analysis, Intelligence Oversight Guidelines* (Washington, D.C.: Jan. 2017).

to ensure that in executing its mission—including intelligence activities related to surface transportation—DHS I&A does not compromise the privacy, civil rights, and civil liberties of U.S. persons when conducting intelligence activities.

TSA and DHS I&A have measures to protect the privacy of persons and companies referenced in intelligence and other information products. For example, according to the instructions accompanying DHS I&A's Intelligence Oversight Guidelines, prior to disseminating information, DHS I&A must take steps to avoid unnecessarily sharing information that is reasonably likely to identify specific U.S. persons or companies by replacing it with a generic marking, such as "U.S. Person."⁶² If DHS I&A determines that sharing the identity of a specific U.S. person or company is necessary for understanding and using the information or intelligence, it must include an advisory indicating that identifying information is contained within the document being disseminated and highlight the individual or company information in a manner that clearly identifies it as such. Similarly, according to TSA's Standard Operating Procedure for Field Information Reports Production, if TSA intelligence staff include information identifying a U.S. person or company in field information reports, they must include an advisory indicating that such information is contained within the report and include the designation next to the individual or company to identify it.⁶³

In addition, TSA and DHS I&A have policies to review intelligence products prior to dissemination, which would include products about surface transportation security threats. Specifically, both entities' processes require review of finished intelligence by multiple offices prior to dissemination (see figure 3).

- TSA's process for producing finished intelligence products calls for reviews by multiple DHS and TSA offices, including DHS's Office of

⁶²Department of Homeland Security, *Office of Intelligence and Analysis, Intelligence Oversight Program and Guidelines*, Instruction IA-1000 (Washington, D.C.: Jan. 19, 2017).

⁶³Transportation Security Administration, *Standard Operating Procedure Field Information Reports Production* (April 2023).

the General Counsel and TSA's Civil Rights and/or Liberties, Ombudsman, and Traveler Engagement.⁶⁴

- Similarly, DHS I&A's policy for producing finished intelligence products requires review by multiple offices before they are disseminated outside of DHS.⁶⁵ Finished intelligence products that include information and analysis relating to U.S. persons, a constitutionally protected activity, or other matters that have significant oversight equities are reviewed by DHS's Office of the General Counsel and Office for Civil Rights and Civil Liberties, among others. These reviews are to serve several purposes, one of which is to help ensure appropriate protections of individuals' privacy, civil rights, and civil liberties.⁶⁶

⁶⁴The review process described here and in the associated figure applied to unclassified finished intelligence. In October 2023, TSA reported that DHS I&A Intelligence Oversight Program Office had recently ceased review of TSA intelligence products because the DHS I&A Intelligence Oversight Guidelines were not mandatory for TSA products. TSA also said that TSA and DHS I&A were discussing if reviews by DHS I&A Intelligence Oversight Program Office were prudent, nonetheless.

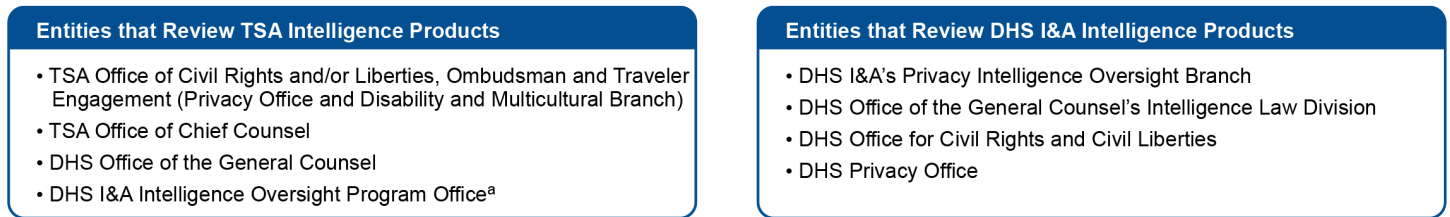
In October 2023, TSA also reported changes to its review process for classified products, which previously were reviewed by TSA's Office of Chief Counsel and DHS's Office of the General Counsel. Starting in October 2023, classified products were to be reviewed by TSA's Civil Rights and/or Liberties, Ombudsman, and Traveler Engagement.

In addition, TSA does not require field information reports, which are raw information reports, to comply with processes used for finished intelligence products because TSA does not consider them intelligence products. However, field information reports are required to be reviewed by supervisory intelligence staff prior to dissemination.

⁶⁵DHS, *Office of Intelligence and Analysis, Office of Intelligence and Analysis Production of Finished Intelligence*, Policy Instruction IA-901 (Revision 3) (Washington, D.C.: Aug. 25, 2022).

⁶⁶These reviews also aim to ensure that DHS I&A's finished intelligence products (1) are issued in a timely manner; (2) conform to I&A's authorized missions, analytic tradecraft and qualitative standards, and legal, policy, and regulatory requirements; (3) respond to the requirements of I&A customers; and (4) maintain the integrity of the intelligence process. DHS I&A, *Office of Intelligence and Analysis, Office of Intelligence and Analysis Production of Finished Intelligence*, Policy Instruction IA-901 (Revision 3) (Washington, D.C.: Aug. 25, 2022)

Figure 3: Offices that Review Transportation Security Administration (TSA) and Department of Homeland Security (DHS) Office of Intelligence and Analysis (I&A) Finished Intelligence Products for Privacy, Civil Rights, and Civil Liberties Issues



Source: GAO analysis of TSA and DHS I&A information. | GAO-24-106382

^aIn October 2023, TSA reported that DHS I&A Intelligence Oversight Program Office had recently ceased review of TSA intelligence products because the DHS I&A Intelligence Oversight Guidelines were not mandatory for TSA products. As of November 2023, TSA officials said TSA and DHS I&A were discussing if reviews by DHS I&A Intelligence Oversight Program Office were prudent and should be continued, nonetheless.

TSA and DHS I&A staff are also required to receive training on privacy, civil rights, and civil liberties protections. For example, all staff are required to complete a module on privacy protections as part of DHS's annual mandatory training. In addition, DHS's Office for Civil Rights and Civil Liberties has delivered a series of training modules to DHS I&A and TSA intelligence staff on the civil rights and civil liberties protections afforded to individuals in the course of collecting intelligence information and generating intelligence products. See figure 4 for more information on our prior work related to DHS I&A's measures intended to protect privacy, civil rights, and civil liberties.

Figure 4: Prior GAO Review of Department of Homeland Security’s (DHS) Office of Intelligence and Analysis (I&A) Implementation of Civil Rights, Civil Liberties, and Privacy Protections

As a member of the Intelligence Community, DHS I&A has additional oversight measures to which its intelligence activities are subject. Specifically, DHS I&A’s Intelligence Oversight Guidelines require that it have an Intelligence Oversight Officer to implement the guidelines and ensure that DHS I&A personnel comply with them.^a To that end, the guidelines and the accompanying policy instruction identify various activities to conduct, including periodic compliance reviews and preliminary inquiries to verify DHS I&A staff’s implementation of the guidelines.

In our August 2023 report, GAO evaluated the extent to which DHS I&A monitored the implementation of these guidelines. We reported that we were not able to confirm that DHS I&A performed periodic compliance reviews between January 2017 and September 2022 because DHS I&A officials did not document all the reviews they said they completed.^b We made recommendations to address this and other issues we identified in that report, and are monitoring DHS I&A’s implementation.

^aDHS I&A’s Intelligence Oversight Officer is to conduct periodic reviews to verify compliance with the DHS I&A Oversight Guidelines—for example, through unannounced “spot checks,” records reviews, or employee and contractor interviews. DHS I&A’s Intelligence Oversight Officer, in consultation with the Associate General Counsel for Intelligence, is to initiate a preliminary inquiry upon notification of any potential violation of federal criminal law or questionable activity. Department of Homeland Security, *Office of Intelligence and Analysis, Office of Intelligence and Analysis Intelligence Oversight Program and Guidelines*, Instruction IA-1000 (Washington, D.C.: Jan. 19, 2017).

^bSee GAO, *Homeland Security: Office of Intelligence and Analysis Should Improve Privacy Oversight and Assessment of Its Effectiveness*, GAO-23-105475 (Washington, D.C.: Aug. 28, 2023).

Source: GAO analysis of DHS I&A information and GAO, *Homeland Security: Office of Intelligence and Analysis Should Improve Privacy Oversight and Assessment of Its Effectiveness*, GAO-23-105475 (Washington, D.C.: Aug. 28, 2023). | GAO-24-106382

Surface Transportation Stakeholders Can Apply for Security Clearances through DHS, but Some Stakeholders and Agency Staff Had Misunderstandings about Some Aspects of Accessing the Process

Surface Transportation Owners and Operators Can Apply for a Security Clearance through Several Federal Entities, Including DHS

Surface transportation owners and operators can apply for a security clearance through one of several federal entities, including DHS and its component agencies, TSA and the Cybersecurity and Infrastructure Security Agency (CISA). TSA, as the lead agency for sharing transportation security information, has granted security clearances for transportation owners and operators—including surface transportation owners and operators—at the secret level.⁶⁷ From fiscal years 2018 through 2023, TSA reported that it initiated 34 to 50 security clearance applications each year for surface transportation owners, operators, and stakeholders, except for fiscal year 2022, when TSA initiated 124 applications (see figure 5).⁶⁸ For the purposes of this report, “initiate” refers to the step in the security clearance application process when the

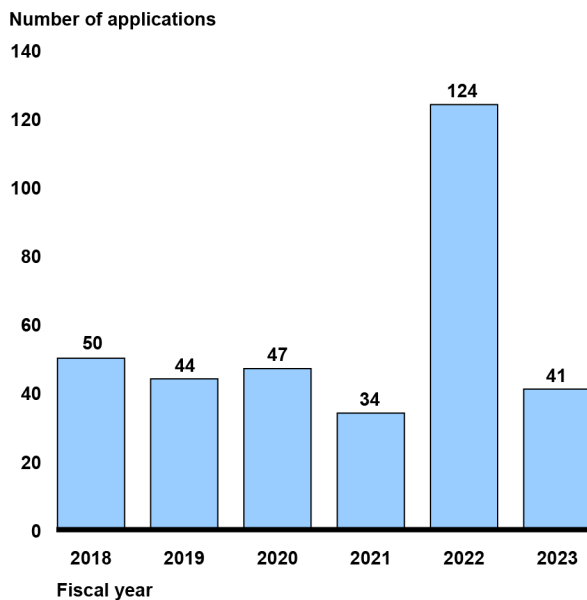
⁶⁷As discussed in further detail below, in 2023, DHS determined that some component agencies—including TSA—had granted security clearances to SLTPS entities without appropriate delegation of authority and, in August 2023, instructed those component agencies to stop granting security clearances.

⁶⁸According to DHS and CISA officials, they were not able to separate surface transportation owners, operators, and stakeholders from among other non-federal applicants in their security clearance data. Specifically, security clearance data for non-federal applicants did not otherwise classify them in a way that would have allowed us to reliably query the data to identify surface transportation stakeholders.

As described in further detail below, TSA’s and CISA’s security clearance processes changed in August 2023. However, those changes did not affect the way applications were initiated.

applicant's information is submitted to the appropriate office for processing. Within TSA, for example, TSA's Office of Policy, Plans, and Engagement initiates the application process by submitting an applicant's information to TSA's Office of Security, Personnel Security Division. Not all initiated applications are granted a security clearance; that determination is made based on the results of the applicant's background investigation.⁶⁹

Figure 5: Number of Security Clearance Applications Initiated by the Transportation Security Administration (TSA) for Surface Transportation Owners and Operators, Fiscal Years 2018 through 2023



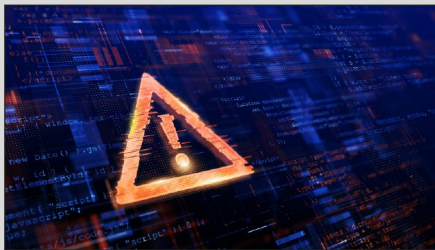
Source: TSA reported data. | GAO-24-106382

Note: For the purposes of this report, "initiate" refers to the step in the security clearance application process when the applicant's information is submitted to the appropriate office for processing. Within TSA, for example, TSA's Office of Policy, Plans, and Engagement initiates the application process by submitting an applicant's information to TSA's Office of Security, Personnel Security Division. Not all initiated applications are granted a security clearance; that determination is made based on the results of the applicant's background investigation.

⁶⁹We provide additional detail about the security clearance application process later in this report.

Cyberattack on Colonial Pipeline

In May 2021, malicious actors used ransomware to conduct a cyberattack against Colonial Pipeline's information technology network, which disrupted gasoline supplies throughout the East Coast. According to the Department of Justice, individuals in a group known as DarkSide were responsible for conducting the cyberattack against Colonial Pipeline's information technology network. Ransomware is malicious software used to deny access to systems or data until a ransom is paid.



Source: Department of Justice; Sashkin/stock.adobe.com. | GAO-24-106382

TSA officials we interviewed attributed the increase in security clearance applications in fiscal year 2022 to two causes:

- First, following the May 2021 Colonial Pipeline cyberattack, TSA released security directives requiring select freight railroad, public transportation and passenger rail, and pipeline owners and operators to take certain steps to enhance the cybersecurity of their assets.⁷⁰ These steps included each owner and operator identifying at least two staff who were eligible for a security clearance to serve as cybersecurity coordinators for liaising with TSA and CISA. According to TSA officials, many of these cybersecurity coordinators subsequently sought security clearances.
- Second, there was an increase in surface transportation owners' and operators' interest in accessing classified intelligence information about nation-state threats following Russia's invasion of Ukraine in February 2022.

In addition, surface transportation owners, operators, and other stakeholders we interviewed reported having security clearances granted by FBI, Department of Defense, and Department of Energy based on the nature of their need for classified information and relationship to the sponsoring agency. For example, according to owners and operators we interviewed, those who participate in FBI Joint Terrorism Task Force activities have been sponsored by FBI, freight rail owners and operators who support the movement of military supplies have been sponsored by the Department of Defense, and pipeline owners and operators reported being sponsored by the Department of Energy.

In 2023, DHS and Component Agency Security Clearance Processes Changed, but Component Agencies Could Still Initiate Applications

In 2023, DHS determined that some component agencies—including TSA and CISA—had granted security clearances to state, local, tribal, and private sector (SLTPS) entities without appropriate delegation of authority. In response, DHS instructed those component agencies to

⁷⁰See TSA, *Security Directives 1580-21-01A (freight railroad)* (Springfield, VA; Oct. 24, 2022); TSA, *1582-21-01A (public transportation and passenger rail)* (Springfield, VA; Oct. 24, 2022), and TSA, *Pipeline-2021-01B (pipeline)* (Springfield, VA; May 29, 2022).

modify their security clearance application processes.⁷¹ Specifically, DHS's Chief Security Officer issued a memo in August 2023 instructing DHS components—including TSA and CISA—to stop granting clearances to SLTPS entities and to work with DHS's Office of the Chief Security Officer because it was the entity with the appropriate authority to grant such clearances.⁷² According to the memo, DHS's Office of the Chief Security Officer intended to request the delegation of authority to permit components to grant clearances under Executive Order 13549 up to the secret level. However, as of October 2023, TSA and CISA officials did not know when DHS's Office of the Chief Security Officer planned to request the delegation of authority.

While DHS's Office of the Chief Security Officer addresses this issue, TSA and CISA cannot grant clearances, though they can initiate applications for SLTPS stakeholders. Surface transportation owners and operators seeking a security clearance may still contact TSA, DHS I&A, or CISA staff to access the security clearance application process in the same manner they did prior to August 2023. Per instructions issued by DHS's Chief Security Officer, while DHS's Office of the Chief Security Officer determines its next steps for delegating authority to permit components to grant clearances, component agencies do not have the authority to adjudicate clearances for SLTPS stakeholders. However,

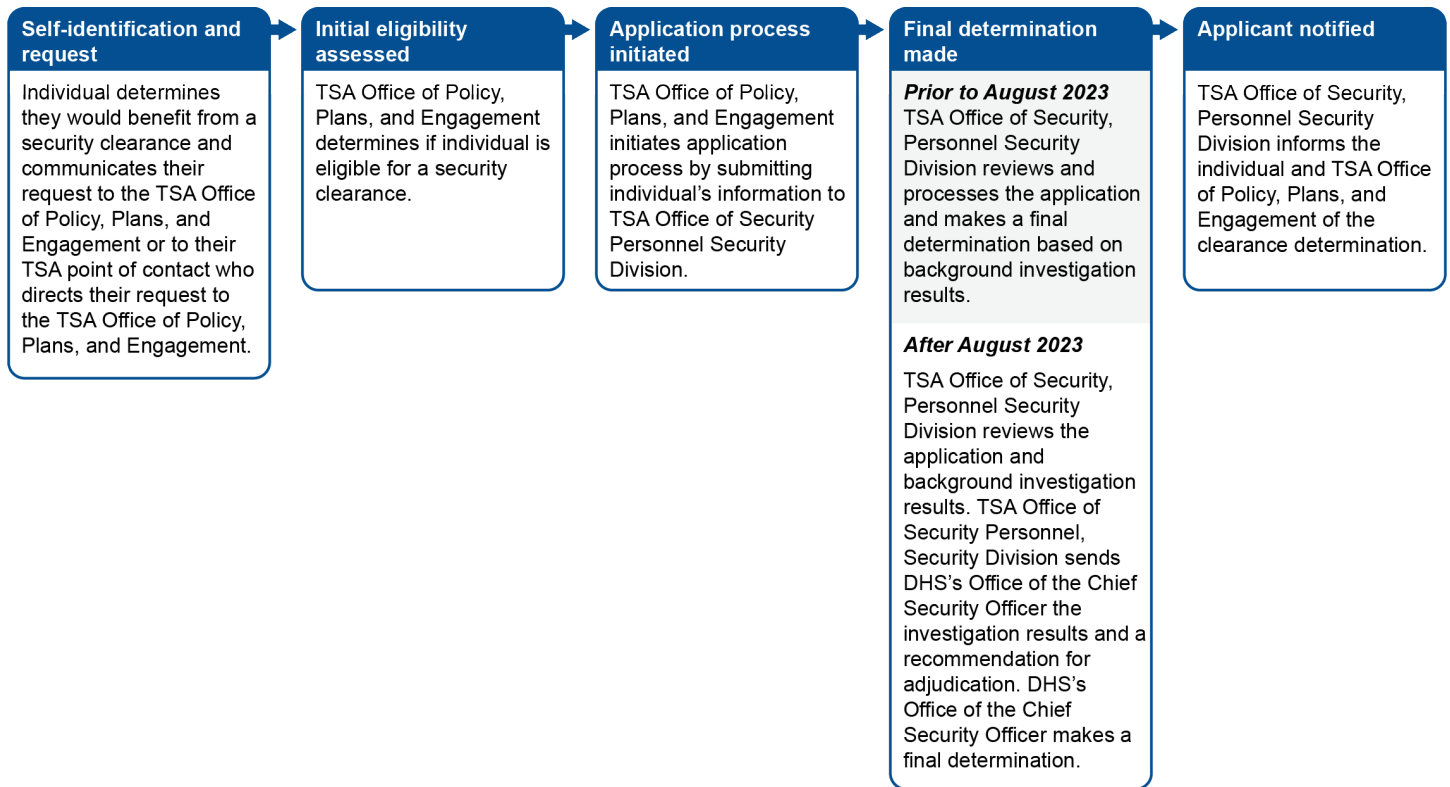
⁷¹Executive Order 13549, *Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities* was intended to ensure that the security standards governing access to and safeguarding of classified material in accordance with all relevant executive orders was uniformly implemented with regards to SLTPS entities. 75 Fed. Reg. 51609 (Aug. 18, 2010). Executive Order 13459 gave DHS the authority to grant security clearances to SLTPS entities, which the Secretary of DHS delegated to the Chief Security Officer via Delegation 12000. The Secretary did not delegate the authority to grant clearances to SLTPS entities under Executive Order 13459 to DHS components. Though DHS issued guidance to components on processing clearances under Executive Order 13459, a memo issued by the Chief Security Officer in August 2023 specified that "such guidance must be read in conjunction with the actual authorities granted within the Department," and that the "the existence of such guidance does not equate to a redelegation of this authority to the Components." DHS, *Memorandum for Component Chief Security Officers: State, Local, Tribal, and Private Sector Personnel Security Clearances Processed Under Executive Order 13459* (Washington, D.C.: Aug. 8, 2023).

⁷²The DHS Office of the Chief Security Officer is a DHS headquarters entity whose mission is to deliver enterprise-wide security solutions to protect DHS's people, information, and resources from evolving threats. The August 2023 memo from the Chief Security Officer also said the DHS Office of the Chief Security Officer would work with each component to ensure that operational impacts are minimized for those clearances adjudicated under the incorrect authority.

TSA, DHS I&A, and CISA can still initiate security clearance applications for SLTPS stakeholders for adjudication by DHS.

From the perspective of SLTPS stakeholders, the process remains unchanged. For example, TSA's SLTPS security clearance application process—including for surface transportation owners and operators—generally starts with the SLTPS stakeholder's determination that they would benefit from a security clearance. The individual may then contact TSA field-based intelligence staff, surface operations staff, or their respective industry engagement manager, all of whom would direct the individual to TSA's Office of Policy, Plans, and Engagement. This office initiates the application, as summarized in figure 6. As of August 2023, at the step where the final determination is made, instead of TSA's Office of Security, Personnel Security Division making the final determination based on the background investigation results, TSA is to forward all investigation materials and adjudication recommendations to DHS's Office of the Chief Security Officer to be make the final determination.

Figure 6: Transportation Security Administration (TSA) Process for Surface Transportation Stakeholders to Apply for a Security Clearance



Source: GAO analysis of Department of Homeland Security Office of the Chief Security Officer and TSA information. | GAO-24-106382

Note: In August 2023, DHS's Chief Security Officer instructed DHS components—including TSA and CISA—to stop granting security clearances to SLTPS entities because it had not appropriately delegated the authority to do so. In that memo, components were instructed to send investigative materials and an adjudicative recommendation to the DHS Office of the Chief Security Officer who has the authority to grant security clearances for the Department. DHS, *Memorandum for Component Chief Security Officers: State, Local, Tribal, and Private Sector Personnel Security Clearances Processed Under Executive Order 13549*, (Washington, D.C.: Aug. 8, 2023).

For SLTPS stakeholders seeking a security clearance through CISA, the process was similarly modified so that DHS's Office of the Chief Security Officer makes the final determination. For example, under CISA's process, designated CISA staff determined if an individual meets the eligibility criteria to be nominated. For surface transportation owners and operators, this would mean individuals who had a need-to-know for the content of classified information to support CISA in protecting critical infrastructure. Prior to August 2023, CISA staff submitted the applicant's information to CISA's Office of the Chief Security Officer for processing. Following the DHS Chief Security Officer's August 2023 memo, CISA is to

submit investigation materials and adjudication recommendations to DHS's Office of the Chief Security Officer to make the final determination instead.

Some Agency Staff and Stakeholders Had Misunderstandings about Some Aspects of Accessing the Security Clearance Application Process

Though DHS and its relevant entities' (TSA, DHS I&A, and CISA) documents described the security clearance application process, agency officials had different understandings of some aspects of their implementation, including which DHS entity was responsible for initiating security clearances for surface transportation owners and operators. The National Defense Authorization Act for Fiscal Year 2022 calls for the Secretary of Homeland Security to make the security clearance application process available to appropriate owners and operators of surface transportation assets to foster greater sharing of relevant classified information.⁷³ DHS entities had policies and processes for SLTPS stakeholders—such as surface transportation owners and operators—to access the security clearance application process. However, agency officials, field-based intelligence staff, and surface transportation stakeholders we interviewed misunderstood how some aspects of those policies were applied, specifically as they related to accessing the security clearance application process. Those misunderstandings may have caused some surface transportation owners and operators to not apply for security clearances.

DHS issued department-wide guidance and DHS I&A, TSA, and CISA each had applicable policies and processes for SLTPS stakeholders to access the security clearance application process. Specifically, in 2012, DHS published an implementing directive intended to establish consistent application of standardized security processes and procedures across the department and its component agencies for managing security clearances, including applications for those clearances. In addition, TSA, DHS I&A, and CISA had documented processes for roles and responsibilities within their respective organization for initiating and processing security clearances.

Though these documents described the security clearance application process, agency officials, field-based intelligence staff, and surface transportation stakeholders we interviewed misunderstood how some aspects of those policies were applied, specifically as they related to accessing the security clearance application process. Specifically, some had different understandings about (1) which DHS entity was responsible

⁷³§ 6418(c), 135 Stat. at 2416.

for initiating applications for surface transportation owners and operators, (2) whether there was a maximum number of security clearances that each would sponsor, and (3) the type of employee—for example, high level executives or security operations staff—eligible for a clearance.

- **Entity responsible for initiating surface transportation stakeholder applications.** Almost half of the TSA field-based staff—intelligence staff and surface inspectors—we interviewed said they would refer interested surface transportation owners and operators to TSA’s Office of Policy, Plans, and Engagement to initiate the security clearance process. Yet, some TSA field-based staff said they referred interested parties to CISA.

For example, in one location, the surface inspector we interviewed said they referred those interested in applying for a security clearance to the local TSA field-based intelligence staff. However, this local field-based intelligence staff told us that they understood CISA was responsible for initiating clearances for surface transportation owners and operators and would refer the interested parties to local CISA staff. Some DHS I&A field-based intelligence staff also reported referring surface transportation owners and operators to CISA for security clearances.

Directing these owners and operators to CISA to access the security clearance process creates confusion because, according to CISA officials, it is not primarily responsible for providing access for surface transportation stakeholders in the security clearance process. According to CISA officials, TSA was primarily responsible for clearances for surface transportation owners and operators because it is the lead agency responsible for sharing information with them and they would rely on TSA to determine the individual’s need for a security clearance.

However, this could also be confusing because a certain subset of surface transportation stakeholders could seek a security clearance through either CISA or TSA. For example, though TSA is the lead agency for surface transportation information sharing, owners and operators of higher-risk surface transportation assets are required to share information about certain cyber events with CISA. This is done to comply with TSA security directives initially issued in 2021 in response to cyber threats to pipelines, railroads, and rail transit

agencies.⁷⁴ According to CISA officials and consistent with CISA’s security clearance guidance, which requires support of CISA’s mission, these particular surface transportation staff could be eligible for a security clearance through CISA.

In addition, CISA officials we interviewed said they understood that DHS I&A was shifting to only sponsoring state and local government officials and not other stakeholders, such as infrastructure owners and operators. However, officials from DHS’s security office said that was not the case.

- **Maximum number of clearances.** Some field-based staff and other stakeholders we interviewed said they understood TSA and CISA had a maximum number of clearances each would grant.⁷⁵ However, headquarters officials from those entities said there were no such caps. Consistent with DHS’s implementing directive of the clearance program, TSA’s and CISA’s policies state that the granting of security clearances should be kept to the “minimum necessary” to support mission activities. According to TSA headquarters officials we interviewed, there is no maximum number of security clearances each agency will grant or maximum number per owner, operator, or other stakeholder entity. They consider each applicant’s need-to-know in the context of their role and their organization.⁷⁶ However, two surface inspectors we interviewed, as well as two owners and operators, and one industry association said that currently, or in the past, TSA limited the number of security clearances it granted for surface transportation owners and operators. According to TSA headquarters officials, these understandings were incorrect.

⁷⁴Higher-risk freight railroads, public transportation and passenger railroads, and pipeline owners and operators are required to report to CISA unauthorized access to information or operational technology systems and the discovery of malicious software on such systems, among other cybersecurity incidents. See TSA, *Security Directives 1580-21-01 (freight railroad)* (Springfield, VA; Dec. 31, 2021); TSA, *1582-21-01 (public transportation and passenger rail)* (Springfield, VA; Dec. 31, 2021), and TSA, *Pipeline-2021-01B (pipeline)* (Springfield, VA; May 29, 2022).

⁷⁵In 2023, DHS determined that some component agencies—including TSA and CISA—had granted security clearances to SLTPS entities without appropriate delegation of authority, and, in August 2023, DHS instructed those component agencies to stop granting security clearances while DHS determined next steps. Field-based staffs’ and other stakeholders’ perspectives described here reflect their understanding of the process prior to the August 2023 instruction from DHS that component agencies stop granting security clearances to SLTPS entities.

⁷⁶According to CISA, its process included questioning CISA sponsors on the need-to-know of SLTPS stakeholders to ensure security clearances were required to support the agency’s mission.

-
- **Type of employee eligible.** Some surface transportation stakeholders also expressed confusion about which types of employees can apply for clearances. For example, one national association and one surface transportation owner and operator indicated that it was their understanding that only top leadership positions at the company, like the chief executive officer, can apply for clearances. TSA officials also told us that some surface transportation stakeholders think that only staff in such leadership positions can apply for clearances, but being in a leadership position is not a requirement for TSA to initiate a security clearance application.

GAO's *Standards for Internal Control in the Federal Government* notes that effective communication is vital for an entity to achieve its objectives. This includes communicating necessary quality information internally and externally. DHS and its relevant entities—TSA, DHS I&A, and CISA—had applicable policies and processes for SLTPS stakeholders to access the security clearance process. However, agency officials, field-based intelligence staff, and surface transportation stakeholders misunderstood how some aspects of those policies were applied, specifically as they related to accessing the security clearance application process. For example, some had different understandings about which DHS entity was responsible for initiating security clearances for surface transportation owners and operators, whether there was a maximum number that could be granted, and the type of employee eligible.⁷⁷

Misunderstandings of key information about accessing the security clearance application process may have caused some surface transportation owners and operators to not apply. For example, some surface transportation owners, operators, and other stakeholders who could benefit from access to classified information may not seek a security clearance because they believe DHS, or its components, would not sponsor them because too many others in their organization already have a clearance. Implementing a coordinated communications approach could help ensure relevant TSA, DHS I&A, and CISA staff, as well as surface transportation stakeholders, have consistent and accurate information about the security clearance application process. This, in turn, will ultimately facilitate classified information sharing when the need arises. Each entity is responsible for ensuring its own staff has accurate

⁷⁷Though TSA's and CISA's policy documents were not wholly applicable following the August 2023 memo from the DHS Chief Security Officer, the primary change was the entity making the final determination; the way surface transportation owners and operators might access the application process were not affected.

information about the security clearance process. Further, as the lead agency for providing transportation security-related information to SLTPS entities, including surface transportation owners and operators, TSA would be best positioned to coordinate the communications approach for sharing information with those owners and operators and other surface transportation stakeholders about accessing the security clearance application process. Given DHS's Office of the Chief Security Officer's ongoing efforts to address issues related to its delegation of authority to components to grant security clearances, TSA, DHS I&A, and CISA may determine it is appropriate to reserve their resources and implement their communication approaches once those issues are resolved.

Though Classified Information-Sharing Has Been Infrequent, Field-Based Intelligence Staff and Stakeholders Generally Agreed Having Security Clearances was Beneficial

Almost all of the 15 field-based intelligence staff and two-thirds of the 15 surface transportation owners and operators we interviewed said surface transportation stakeholders having security clearances was beneficial to information sharing, even though nearly two-thirds of those field intelligence staff said they had not shared or rarely shared classified information with surface transportation stakeholders during the time period about which we inquired. Most field-based intelligence staff and surface transportation owners and operators we interviewed said there were benefits to surface transportation owners and operators having security clearances. TSA and DHS I&A field-based intelligence staff stated that they have not frequently needed to share classified information with surface transportation owners, operators, and other stakeholders. According to field-based intelligence staff, that is because specific threats to surface transportation assets were not common and field-based intelligence staff could generally disseminate relevant information at the unclassified level.

Nearly two-thirds of the field-based intelligence staff we interviewed (9 of 15) said they had not shared or rarely shared classified information with surface transportation stakeholders during the time period we inquired about—fiscal years 2018 through 2023. Among the five field-based intelligence staff who described sharing classified information, the frequency ranged from twice a year to monthly.⁷⁸ For example, one of the field-based intelligence staff said that since the pandemic started in 2020, he has only briefed classified cybersecurity information related to the Russian war in Ukraine to a few surface operators and owners. Surface

⁷⁸One field-based intelligence staff person did not provide information on the frequency of classified information-sharing.

transportation owners and operators we interviewed generally confirmed they did not frequently receive classified information.

Nevertheless, TSA and DHS I&A officials, as well as 14 of 15 TSA and DHS I&A field-based intelligence staff and 11 of the 15 surface transportation owners and operators we interviewed said there were benefits to surface transportation owners and operators having security clearances. Several of these TSA and DHS I&A field-based intelligence staff and owners and operators described a security clearance as beneficial for contingencies. They said that if time-sensitive, classified security information needed to be shared, having surface transportation owners and operators with active security clearances ready to receive the information would facilitate and expedite the process.

Conclusion

The U.S. surface transportation system moves billions of passengers and millions of tons of goods each year. Securing it requires the coordination of several federal entities, state and local law enforcement, and public and private sector owners and operators of surface transportation assets. That coordination includes effective sharing of information about potential threats, which at times may only be conveyed in classified form. According to TSA and DHS I&A officials, field-based intelligence staff, and owners, operators, and other stakeholders we interviewed stated that having a security clearance would enable sharing with relevant parties if the need arose. DHS and its entities—TSA, DHS I&A, and CISA—had policies and processes for non-federal stakeholders, such as surface transportation owners and operators, to access the security clearance application process.

However, agency officials, field-based intelligence staff, and stakeholders we interviewed had different understandings about which DHS entity was responsible for initiating security clearances for surface transportation owners and operators, whether there was a maximum number that could be granted, and the type of employee eligible. Implementing a coordinated communications approach could help ensure relevant TSA, DHS I&A, and CISA staff, as well as surface transportation stakeholders, have consistent and accurate information about accessing the security clearance application process and could help ensure all have important surface transportation security information when needed. Each entity is responsible for ensuring its own staff has accurate information about the security clearance process. Further, as the lead agency for providing transportation security-related information to SLTPS entities, including surface transportation owners and operators, TSA would be best positioned to coordinate the communications approach for sharing

information with those owners and operators and other surface transportation stakeholders about accessing the security clearance application process.

Recommendations for Executive Action

The TSA Administrator, in coordination with DHS I&A, CISA, and DHS's Office of the Chief Security Officer, should implement a communications approach that conveys consistent and accurate information to TSA staff who interact with surface transportation stakeholders about how those stakeholders access the security clearance application process. At minimum, the approach should aim to ensure accurate information about which DHS entities initiate applications for surface transportation stakeholders, whether there is a maximum number of clearances that could be granted, and what type of employees are eligible. (Recommendation 1)

The DHS Under Secretary for Intelligence and Analysis, in coordination with TSA, CISA, and DHS's Office of the Chief Security Officer, should implement a communications approach that conveys consistent and accurate information to DHS I&A staff who interact with surface transportation stakeholders about how those stakeholders access the security clearance application process. At minimum, the approach should aim to ensure accurate information about which DHS entities initiate applications for surface transportation stakeholders, whether there is a maximum number of clearances that could be granted, and what type of employees are eligible. (Recommendation 2)

The CISA Director, in coordination with DHS I&A, TSA, and DHS's Office of the Chief Security Officer, should implement a communications approach that conveys consistent and accurate information to CISA staff who interact with surface transportation stakeholders about how those stakeholders access the security clearance application process. At minimum, the approach should aim to ensure accurate information about which DHS entities initiate applications for surface transportation stakeholders, whether there is a maximum number of clearances that could be granted, and what type of employees are eligible. (Recommendation 3)

The TSA Administrator, in coordination with DHS I&A, CISA, and DHS's Office of the Chief Security Officer, should implement a communications approach that conveys consistent and accurate information to surface transportation stakeholders about how they access the security clearance application process. At minimum, the approach should aim to ensure accurate information about which DHS entities initiate applications for

surface transportation stakeholders, whether there is a maximum number of clearances that could be granted, and what type of employees are eligible. (Recommendation 4)

Agency Comments

We provided a draft of this report to DHS for its review and comment. In its comments, reproduced in full in appendix II, DHS concurred with each of our four recommendations and described actions to address them.

To address our first, second, and third recommendations intended to ensure TSA, DHS I&A, and CISA staff have consistent and accurate information about how surface transportation stakeholders can access the security clearance application process, each entity described planned actions. For example, TSA and DHS I&A officials stated they plan to coordinate with relevant DHS offices to develop consistent information, communications procedures, or guides for staff working with surface transportation stakeholders. CISA noted that it finalized instructions for SLTPS security clearances in May 2023 to help provide consistent information to CISA staff. Though updated guidance is a key step, effective communication with CISA staff that is coordinated with the other relevant DHS entities is necessary to ensure those staff convey consistent and accurate information to surface transportation stakeholders. Given DHS's Office of the Chief Security Officer's ongoing efforts to address issues related to its delegation of authority to components to grant security clearances, GAO will monitor TSA's, DHS I&A's, and CISA's efforts to address these recommendations after such potential policy changes are implemented to ensure that these entities provide consistent and accurate information to their staff.

To address our fourth recommendation intended to ensure consistent and accurate information for surface transportation stakeholders, TSA plans to develop a communication package to inform surface transportation stakeholders of the process and parameters for accessing a security clearance through TSA's program and other similar programs administered by DHS.

DHS also provided technical comments on our draft report, which we incorporated, as appropriate.

We are sending copies of this report to the appropriate congressional committees, the Secretary of Homeland Security, and other interested parties. In addition, the report is available at no charge on the GAO website at <https://www.gao.gov>.

If you or your staff have any questions about this report, please contact Triana McNeil at (202) 512-8777 or McNeilT@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix III.

A handwritten signature in black ink, appearing to read "Triana McNeil". The signature is fluid and cursive, with a large initial "T" and "M".

Triana McNeil
Director, Homeland Security and Justice

Appendix I: Field-Based Intelligence Staffing in Locations with Higher-Risk Surface Transportation Assets for Fiscal Year 2023

This appendix provides additional details about the number of Transportation Security Administration (TSA) and Department of Homeland Security (DHS) Office of Intelligence and Analysis (I&A) field-based intelligence staff by location and type of higher-risk surface transportation asset for fiscal year 2023. In fiscal year 2023, there were a total of 62 geographic areas with at least one higher-risk surface transportation asset—that is, a higher-risk public transportation and passenger railroad system, over-the-road bus operations, or a freight railroad or pipeline company headquarters.¹ Seventeen of these geographic areas had more than one type of higher-risk surface transportation asset. Given TSA’s definitions of higher-risk surface transportation assets, public transportation and passenger railroad systems and over-the-road bus operations are in larger metropolitan areas. Freight railroad and pipeline companies with higher-risk assets have headquarters in a range of locations, including large metropolitan areas and smaller rural areas.

Table 5 shows the location and type of higher-risk surface transportation assets for fiscal year 2023. The 17 locations with multiple higher-risk surface transportation assets are listed first.

Table 5: Location and Type of Higher-Risk Surface Transportation Asset, Fiscal Year 2023

Location	Public transportation/ passenger railroads	Over-the-road bus service	Freight railroad company headquarters	Pipeline system company headquarters
Chicago, IL area	X	X	X	X
New York City-Northern New Jersey area	X	X	X	X
Philadelphia/Southern New Jersey area	X	X	X	X
San Francisco Bay area	X	X	X	X
Atlanta, GA area	X	—	X	X
Boston, MA area	X	X	—	X
Dallas-Fort Worth-Arlington area	—	X	X	X
Greater Los Angeles, CA area	X	X	—	X
Greater Washington D.C./National Capital region	X	X	—	X
Houston, TX area	—	X	X	X

¹85 Fed. Reg. 16,456 (Mar. 23, 2020) (describing a higher-risk operation as one that meets the criteria in 49 C.F.R. §§ 1582.101 (public transportation system and passenger railroads), 1580.101 (freight railroads), and 1584.101 (over-the-road buses)).

**Appendix I: Field-Based Intelligence Staffing in
Locations with Higher-Risk Surface
Transportation Assets for Fiscal Year 2023**

Location	Public transportation/ passenger railroads	Over-the-road bus service	Freight railroad company headquarters	Pipeline system company headquarters
Indianapolis, IN area	—	—	X	X
Madison, WI	—	—	X	X
New Orleans, LA area	—	—	X	X
Omaha, NE area	—	—	X	X
Portland, OR area	—	—	X	X
St. Louis, MO area	—	—	X	X
San Diego, CA area	—	X	—	X
Albuquerque, NM	—	—	—	X
Allentown, PA	—	—	—	X
Anchorage, AK	—	—	—	X
Bismarck, ND	—	—	—	X
Brewster, OH	—	—	X	—
Buffalo, NY area	—	—	—	X
Burlington, VT area	—	—	X	—
Carthage, MO	—	—	X	—
Casper, WY	—	—	—	X
Cedar Rapids, IA	—	—	X	—
Charlotte, NC area	—	—	—	X
Covington, LA	—	—	—	X
Denver, PA	—	—	—	X
Des Moines, IA area	—	—	—	X
Detroit, MI area	—	—	—	X
Dillwyn, VA	—	—	X	—
Dover, DE	—	—	—	X
Fayetteville, NC	—	—	—	X
Findlay, OH	—	—	—	X
Folsom, NJ	—	—	—	X
Jackson, MI	—	—	—	X
Jacksonville, FL area	—	—	X	—
Kansas City, MO area	—	—	X	X
Las Vegas, NV area	—	—	—	X
Louisville, KY area	—	—	—	X
Memphis, TN area	—	—	—	X
Michigan City, IN	—	—	X	—
Owensboro, KY	—	—	—	X
Paducah, KY	—	—	X	—

**Appendix I: Field-Based Intelligence Staffing in
Locations with Higher-Risk Surface
Transportation Assets for Fiscal Year 2023**

Location	Public transportation/ passenger railroads	Over-the-road bus service	Freight railroad company headquarters	Pipeline system company headquarters
Pittsburgh, PA area	—	—	—	X
Port Huron, MI	—	—	—	X
Portage, MI	—	—	—	X
Rapid City, SD	—	—	—	X
Richmond, VA	—	—	—	X
Rochester, NY	—	—	X	—
Salem, OR	—	—	X	—
Salt Lake City, Utah	—	—	—	X
San Antonio, TX area	—	—	—	X
Seattle, WA area	—	—	—	X
Shelton, CT	—	—	—	X
Spokane, WA	—	—	—	X
Tampa, FL area	—	—	—	X
Tulsa, OK	—	—	—	X
Twin Cities, MN area	—	—	—	X
Wichita, KS	—	—	—	X
Total	8	10	24	52

Legend: X = Presence of higher-risk surface transportation asset type in the identified area. — = No higher-risk surface transportation asset type in the identified area.

Source: GAO analysis of Transportation Security Administration data. | GAO-24-106382

Notes: In fiscal year 2023, there were a total of 62 geographic areas with at least one higher-risk surface transportation asset.

Totals in each column will not sum to 62 because 17 locations had more than one mode of higher-risk surface transportation asset.

TSA and DHS I&A allocated their respective field-based intelligence staff to locations across the country, including many of the 62 geographic areas with higher-risk surface transportation assets, or in their general proximity. TSA field-based intelligence staff are located at airports and are to provide intelligence support to TSA entities and external stakeholders for all modes of transportation, including surface transportation. DHS I&A generally assigns field-based intelligence staff to one of the nation’s 80 fusion centers, where they provide intelligence support to state, local, tribal, territorial, and private sector stakeholders

Appendix I: Field-Based Intelligence Staffing in Locations with Higher-Risk Surface Transportation Assets for Fiscal Year 2023

and decisionmakers at all levels.² Table 6 shows TSA and DHS I&A staffing information for locations with higher-risk surface transportation assets, by location for fiscal year 2023. The 17 locations with multiple higher-risk surface transportation assets are listed first.

For the purposes of this report, field-based intelligence staff were determined to be in the same geographic area as the higher-risk surface transportation asset if the airport or fusion center to which the staff were allocated was within the same geographic area as the assets or operations described in 49 C.F.R. §§ 1580.101, 1582.101, 1584.101. For higher-risk surface transportation assets in locations other than those described in the cited regulations, field-based intelligence staff were determined to be in the same geographic area if the airport or fusion center to which the staff were allocated were within an approximately 10-mile buffer area around the city where the asset was located. We used the 10-mile buffer area to correspond with the 10-mile buffer area applied to high threat urban areas in federal regulations.³

The table does not include locations without higher-risk surface transportation assets where TSA and DHS I&A have allocated staff.

Table 6: Transportation Security Administration (TSA) and Department of Homeland Security (DHS) Office of Intelligence and Analysis (I&A) Staffing in Locations with Higher-Risk Surface Transportation Assets, by Location for Fiscal Year 2023

Location	Number of field-based intelligence staff allocated			
	TSA on-board	TSA vacant	DHS I&A on-board	DHS I&A vacant
Chicago, IL area	2	0	1	0
New York City-Northern New Jersey area	3	0	2	0
Philadelphia/Southern New Jersey area	1	0	1	1
San Francisco Bay area	3	0	1	0
Atlanta, GA area	1	0	1	0
Boston, MA area	0	1	2	0
Dallas-Fort Worth-Arlington area	1	0	2	1

²Two field-based intelligence staff are assigned locations in New York City where there is no fusion center. State governors designate fusion centers, which are owned and operated by state and local entities. New York has designated a primary fusion center located in its capital, Albany; it does not have any regional fusion centers.

³49 C.F.R. § 1580.101, App. A (noting that “a 10-mile buffer extending from the border of the combined area” is included in the geographic areas for all High Threat Urban Areas).

**Appendix I: Field-Based Intelligence Staffing in
Locations with Higher-Risk Surface
Transportation Assets for Fiscal Year 2023**

Location	Number of field-based intelligence staff allocated			
	TSA on-board	TSA vacant	DHS I&A on-board	DHS I&A vacant
Greater Los Angeles, CA area	3	0	2	0
Greater National Capital Region	4	0	2	0
Houston, TX area	2	0	1	0
Indianapolis, IN area	1	0	1	0
Madison, WI	0	0	1	0
New Orleans, LA area	0	1	0	0
Omaha, NE area	1	0	0	0
Portland, OR area	1	0	0	0
St. Louis, MO area	1	0	1	0
San Diego, CA area	0	1	1	0
Albuquerque, NM	0	0	0	0
Allentown, PA	0	0	0	0
Anchorage, AK	1	0	1	0
Bismarck, ND	0	0	0	1
Brewster, OH	0	0	0	0
Buffalo, NY area	0	0	0	0
Burlington, VT area	0	0	1	0
Carthage, MO	0	0	0	0
Casper, WY	0	0	0	0
Cedar Rapids, IA	0	0	0	0
Charlotte, NC area	1	0	0	0
Covington, LA	0	0	0	0
Denver, PA	0	0	0	0
Des Moines, IA area	0	0	1	0
Detroit, MI area	1	0	1	0
Dillwyn, VA	0	0	0	0
Dover, DE	0	0	1	0
Fayetteville, NC	0	0	0	0
Findlay, OH	0	0	0	0
Folsom, NJ	0	0	0	0
Jackson, MI	0	0	0	0
Jacksonville, FL area	1	0	0	0
Kansas City, MO area	1	0	1	0
Las Vegas, NV area	1	0	1	0
Louisville, KY area	0	0	0	0

**Appendix I: Field-Based Intelligence Staffing in
Locations with Higher-Risk Surface
Transportation Assets for Fiscal Year 2023**

Location	Number of field-based intelligence staff allocated			
	TSA on-board	TSA vacant	DHS I&A on-board	DHS I&A vacant
Memphis, TN area	1	0	0	0
Michigan City, IN	0	0	0	0
Owensboro, KY	0	0	0	0
Paducah, KY	0	0	0	0
Pittsburgh, PA area	1	0	1	0
Port Huron, MI	0	0	0	0
Portage, MI	0	0	0	0
Rapid City, SD	0	0	0	0
Richmond, VA	0	0	1	0
Rochester, NY	0	0	0	0
Salem, OR	0	0	1	0
Salt Lake City, Utah	1	0	0	1
San Antonio, TX area	1	0	1	0
Seattle, WA area	1	0	1	0
Shelton, CT	0	0	0	0
Spokane, WA	1	0	0	0
Tampa, FL area	1	0	0	0
Tulsa, OK	0	0	0	0
Twin Cities, MN area	2	0	1	0
Wichita, KS	0	0	0	0
Total	39	3	32	4

Source: GAO analysis of TSA and DHS I&A data. | GAO-24-106382

Notes: "Allocated" refers to staff positions for which TSA or DHS I&A have approved funding and assigned to a location.
 "On-board" refers to positions to which TSA or DHS I&A have hired staff; otherwise, the position is considered "vacant."

Appendix II: Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528



**Homeland
Security**

January 19, 2024

Triana McNeil
Director, Homeland Security & Justice
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548-0001

Re: Management Response to Draft Report GAO-24-106382, "SURFACE TRANSPORTATION THREATS: Better Communication with Stakeholders Needed about the Security Clearance Process"

Dear Ms. McNeil:

Thank you for the opportunity to comment on this draft report. The U.S. Department of Homeland Security (DHS or the Department) appreciates the U.S. Government Accountability Office's (GAO) work in planning and conducting its review and issuing this report.

DHS leadership is pleased to note GAO's recognition that the U.S. surface transportation system is a complex system comprising multiple modes of transportation which are often interconnected and operate in close coordination with one another. Accordingly, the threat intelligence information-sharing process is designed to communicate actionable information on threats and incidents in the freight rail, highway and motor carrier, mass transit and passenger rail, maritime, and pipeline modes so that all levels of government, surface transportation owners and operators, and other security partners can assess risks, make security investments, and take protective actions, as appropriate.

Specifically, DHS and the Transportation Security Administration (TSA) allocate dedicated resources to:

- Analyze and assess surface transportation security threats and risks;
- Develop all-source intelligence information;
- Vet intelligence information products in accordance with DHS' and TSA's commitment to privacy and civil liberties; and
- Share surface transportation intelligence information in a timely manner via established mechanisms, including deployment of field-based intelligence staff to geographic areas with higher-risk surface transportation assets.

**Appendix II: Comments from the Department
of Homeland Security**

As part of efforts to foster greater sharing of relevant classified information, DHS Components facilitate surface transportation owners and operators access to the security clearance application process and assist in obtaining security clearances, as appropriate. DHS remains committed to ensuring that surface transportation stakeholders understand processes for obtaining security clearances, and that DHS Office of Intelligence and Analysis (I&A), TSA, and the Cybersecurity and Infrastructure Security Agency (CISA) have clear policies and processes in place for appropriate stakeholders to access the security clearance application process.

The draft report contained four recommendations with which the Department concurs. Enclosed find our detailed response to each recommendation. DHS previously submitted technical comments addressing several accuracy, contextual, and other issues under a separate cover for GAO's consideration.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Sincerely,

**JIM H
CRUMPACKER**

Digitally signed by JIM H
CRUMPACKER
Date: 2024.01.19 15:41:20
-05'00'

JIM H. CRUMPACKER, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

Enclosure

**Enclosure: Management Response to Recommendations
Contained in GAO-24-106382**

GAO recommended that the TSA Administrator, in coordination with DHS I&A, CISA, and DHS's Office of the Chief Security Officer (OCSO):

Recommendation 1: Implement a communications approach that conveys consistent and accurate information to TSA staff who interact with surface transportation stakeholders about how those stakeholders access the security clearance application process. At minimum, the approach should aim to ensure accurate information about which DHS entities initiate applications for surface transportation stakeholders, whether there are maximum numbers of clearances TSA will grant, and what type of employees are eligible.

Response: Concur. TSA's Chief Security Office (CSO) and Policy, Plans, and Engagement (PPE) agree with the importance of having clear guidance to TSA staff to ensure uniform application of a process to assist eligible surface transportation stakeholders, as well as other forms of transportation, in obtaining security clearances. The Chief Security Officer and Assistant Administrator for PPE will work with appropriate TSA offices to review current processes, update guidelines as needed, and remind offices of their roles, responsibilities, and procedures in relevant management documents. The Chief Security Officer and Assistant Administrator for PPE will also work with DHS OCSO and other appropriate DHS offices to:

- Establish a unified, consistent program for TSA staff who interact with surface transportation stakeholders about how they access the security clearance application process; and
- Develop communication procedures for surface transportation stakeholders who manage personnel security clearances.

Estimated Completion Date (ECD): October 31, 2024.

GAO recommended that the Under Secretary for I&A, in coordination with TSA, CISA, and DHS's OCSO:

Recommendation 2: Implement a communications approach that conveys consistent and accurate information to DHS I&A staff who interact with surface transportation stakeholders about how those stakeholders access the security clearance application process. At minimum, the approach should aim to ensure accurate information about which DHS entities initiate applications for surface transportation stakeholders, whether

there are maximum numbers of clearances DHS will grant, and what type of employees are eligible.

Response: Concur. I&A, acting through its Mission Assurance Division, will work with TSA, CISA, and DHS's OCSO, as appropriate to create a guide for I&A staff who interact with surface transportation stakeholders that explains how those stakeholders can access the security clearance application process. This guide will also include information about which DHS entities initiate applications for surface transportation stakeholders, whether DHS will grant a maximum number of clearances, and what types of employees are eligible. ECD: April 30, 2024.

GAO recommended that the CISA Director, in coordination with DHS I&A, TSA, and DHS's OCSO:

Recommendation 3: Implement a communications approach that conveys consistent and accurate information to CISA staff who interact with surface transportation stakeholders about how those stakeholders access the security clearance application process. At minimum, the approach should aim to ensure accurate information about which DHS entities initiate applications for surface transportation stakeholders, whether there are maximum numbers of clearances CISA will grant, and what type of employees are eligible.

Response: Concur. It is important to note that CISA has an existing communications approach for a security clearance application process for critical infrastructure partners, including surface transportation stakeholders. As the National Coordinator for all 16 critical infrastructure sectors and the Sector Risk Management Agency for eight of these sectors, CISA's OCSO, in coordination with CISA's Stakeholder Engagement Division transportation sector lead provides established processes and partnerships for state, local, tribal, and private-sector (SLTPS) security clearance processing.

Specifically, on May 5, 2023, CISA finalized Instruction 3500-01-001, "Sponsoring State, Local, Tribal, and Private Sector (SLTPS) Security Clearances," outlining the process for identifying and submitting SLTPS personnel for security clearances. Additionally, CISA's Office of External Affairs routinely communicates information on its website, and with all 16 critical infrastructure sectors, including the Sector Risk Management Agencies, Government Coordinating Councils, Sector Coordinating Councils, and other partners on all matters regarding critical infrastructure, including requests for or information about security clearances.

We request that GAO consider this recommendation resolved and closed, as implemented.

**Appendix II: Comments from the Department
of Homeland Security**

GAO recommended that the TSA Administrator, in coordination with DHS I&A, CISA, and DHS's OCSO:

Recommendation 4: Implement a communications approach that conveys consistent and accurate information to surface transportation stakeholders about how they access the security clearance application process. At minimum, the approach should aim to ensure accurate information about which DHS entities initiate applications for surface transportation stakeholders, whether there are maximum numbers of clearances DHS entities will sponsor, and what type of employees are eligible.

Response: Concur. TSA's PPE has communicated with the appropriate surface transportation stakeholders to apprise them of the availability of a means to obtain security clearances. In addition, with guidance from the TSA CSO, PPE will develop a communication package to inform surface and other transportation stakeholders of the process and parameters (for example, eligibility, limits, points of contact) for the TSA stakeholder security clearance program and other similar programs administered by DHS. ECD: January 31, 2025.

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Triana McNeil at (202) 512-8777 or McNeilT@gao.gov.

Staff Acknowledgments

In addition to the contacts named above, Erin O'Brien (Assistant Director), Jessica Wintfeld (Analyst in Charge), Benjamin Crossley, Dale Dominick, Brian Lipman, Amanda Miller, Evalin Olson, Ananya Prakash, Mary Turgeon, and Derika Weddington made significant contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its [website](#) newly released reports, testimony, and correspondence. You can also [subscribe](#) to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <https://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#).
Subscribe to our [RSS Feeds](#) or [Email Updates](#). Listen to our [Podcasts](#).
Visit GAO on the web at <https://www.gao.gov>.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: <https://www.gao.gov/about/what-gao-does/fraudnet>

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548

