OFFICE OF INSPECTOR GENERAL

Testimony of Acting Inspector General John V. Kelly

Before the Subcommittee on Surface Transportation and Merchant Marine Infrastructure, Safety, and Security

Committee on Commerce, Science, and Transportation

United States Senate

"Surface Transportation Security: Addressing Current and Emerging Threats"

Homeland Security

February 23, 2018
2:30 PM

Chairman Fischer, Ranking Member Peters, and members of the Subcommittee, thank you for inviting me to testify at today's hearing regarding the security of our surface transportation security.

When the American public thinks of TSA, they think of the Transportation Security Officer in a blue shirt instructing them to remove their belts and shoes before going through security screening at the airport. The truth is that TSA has a much broader responsibility to also oversee and regulate our Nation's surface transportation modes — highway, freight and passenger rail, mass transit, and pipelines — to ensure the freedom of movement for people and commerce. Recent history — the October 2015 bombing of a railway station in Ankara, Turkey; the March 2016 metro bombing in Brussels, Belgium; and the April 2017 metro bombing in St. Petersburg, Russia — depicts how vulnerable surface transportation can be. However, TSA's budget reflects the public perception of its mission, allocating most of its resources to air passenger screening and dedicating only a small portion to these vulnerable areas of non-aviation.

In 2016, the OIG published three reports[1] that identify significant weaknesses in TSA's ability to secure surface transportation modes and the Nation's maritime facilities and vessels. Specifically, we identified issues with TSA's ability to identify risk across all modes of transportation, the reliability of background checks for port workers, and passenger rail security.

TSA Needs a Crosscutting Risk-Based Security Strategy

TSA has many responsibilities beyond air travel, and is responsible, generally through the use of regulation and oversight, for surface transportation security. However, TSA focuses primarily on air transportation security and largely ignores other modes. We found that TSA does not have an intelligence-driven, risk-based security strategy to inform security and budget needs across all types of transportation.

In 2011, TSA began publicizing that it uses an "intelligence-driven, risk-based approach" across all transportation modes. However, we found this not to be true. In an audit we released in September 2016, we reported that TSA specifically designed this approach to replace its one-size-fits-all approach to air passenger screening but did not apply it to other transportation modes. Additionally, TSA's agency-wide risk management organizations provide little oversight of TSA's surface transportation security programs. TSA established

[1] *TSA Oversight of National Passenger Rail System Security* (OIG-16-91); *TWIC Background Checks are Not as Reliable as They Could Be* (OIG-16-128); and *Transportation Security Administration Needs a Crosscutting Risk-Based Security Strategy* (OIG-16-134).

an Executive Risk Steering Committee charged with creating a crosscutting, risk-based strategy, which would drive resource allocations across all modes. However, neither it, nor any of these entities place much emphasis on non-air transportation modes.

In September 2017, TSA reported that it created a crosscutting risk-based strategy based on our recommendations and expected to finalize the strategy in October 2017. However, TSA did not submit this strategy to the OIG. Instead, in January 2018, TSA reported that it intends to submit its pending 2018 National Strategy for Transportation Security (NSTS) as its response to our recommendation for a crosscutting risk-based security strategy. The 2018 NSTS is due to Congress on April 1, 2018 and TSA expects to provide us with a copy by the same date.

We also reported that TSA lacked a formal process to incorporate risk into its budget formulation decisions. Despite the disparate requirements on the agency, TSA dedicated 80 percent of its nearly $7.4 billion FY 2015 budget to direct aviation security expenditures, and only about 2 percent to direct surface transportation expenditures. Its remaining resources were spent on support and intelligence functions. We recommended that TSA establish a formal budget planning process that uses risk to help inform resource allocations.

In September 2017, TSA provided documentation of the steps it has taken to establish a formal budget process that incorporates risk. This includes the development of a formal Planning, Programming, Budgeting, and Execution framework, standing up the Planning and Programming Analysis Branch, and creating five resource portfolios that, among other things, prioritize mission needs across the agency. However, we cannot close this recommendation until we receive TSA's risk-based security strategy and ensure that the strategy's guidelines for aligning resources with risk correspond with its new budget process.

TSA Missing Key Controls within the TWIC Background Check Process

TSA — responsible for safeguarding our Nation's ports and maritime facilities through the Transportation Worker Identification Credential (TWIC) program — lacks key internal controls and this compromises the TWIC program's reliability. These weaknesses leave our Nation's seaports at risk for terrorist exploitation, smuggling, insider threats, and internal conspiracies.

TSA provides background checks, or security threat assessments, for individuals who need unescorted access to secure port facilities; and issues a biometric identification card, also known as a TWIC. The background check

process for TWICs is the same as that of aviation workers[2] and drivers who need a Hazmat Materials Endorsement.[3] It includes a check for immigration-, criminal-, and terrorism-related offenses that would preclude someone from being granted unescorted access to secure facilities at seaports.

In 2011, the Government Accountability Office (GAO) identified key internal control weaknesses in TSA's management of the TWIC background check process and recommended the Department take significant steps to improve the effectiveness of the program as a whole.[4] Although TSA took some steps to address GAO's concerns, our review — five years later — found that TSA did not adequately integrate the security measures intended to identify fraudulent applications into the background check process. For example, TSA required enrollment staff to use a digital scanner that could evaluate security features present on identification documents and generate a score to help TSA determine if the document was authentic. However, TSA did not collect or use these scores when completing its background checks — nullifying the effectiveness of this security measure. For those documents that could not be electronically scanned, TSA required the staff at the enrollment centers to manually review identity documents. However, TSA did not require that the staff be trained at detecting fraudulent documents. When the enrollment staff documented their observations of suspicious identity documents in TSA's system, TSA did not have a standardized process for collecting, reviewing, or using the notes when completing the background checks.

We determined TSA management's lack of oversight was the primary reason the TWIC background check process had many control weaknesses. At the time of our review, the TWIC background check process was divided among multiple program offices so that no single entity had complete oversight and authority over the program. In addition, the TWIC program lacked key metrics to measure TSA's success in achieving program core objectives. For example, the measures in place focused on customer service, such as enrollment time and help desk response time, rather than the accuracy of the background check itself.

As of November 2016, TSA realigned its operations and assigned the Assistant Administrator for the Office of Intelligence and Analysis as the single point of accountability within TSA for the TWIC program's management and operations with the functional oversight over all of the security threat assessment process.

---

[2] *TSA Can Improve Aviation Worker Vetting* (OIG-15-98)

[3] Commercial drivers required to transport hazardous materials must undergo a background check by TSA prior to receiving a hazardous material endorsement on their Commercial Driver's License.

[4] *Transportation Worker Identification Credential: Internal Control Weaknesses Need to be Corrected to Help Achieve Security Objectives* (GAO-11-657).

Additionally, since our review, TSA completed a comprehensive risk analysis that reviewed existing controls, identified and analyzed risks, and promoted control activities. TSA is in the process of addressing the concerns identified by the study. TSA also updated its program charter and objectives to focus on (1) efforts to positively verify the identity of applicants; (2) conduct of the TSA Security Threat Assessment; and (3) actions to recurrently vet and revoke TWIC validity. TSA intends to update its performance metrics to better align with the revised objectives. We will continue to monitor TSA's progress in implementing corrective actions to strengthen the TWIC program.

TSA Delays Implementing Passenger Rail Security Regulations

TSA has failed to develop and implement regulations governing passenger rail security required more than nine years ago by the *Implementing Recommendations of the 9/11 Commission Act of 2007* (*9/11 Act*).[5] Unlike the security presence that TSA provides air passengers in airports, its responsibility for rail passengers rests in assessing intelligence, sharing threat information with industry stakeholders, developing industry best practices, and enforcing regulations. This is particularly important due to the volume of passengers using this mode of transportation and the unique challenges in the rail environment.

In fiscal year 2015 alone, Amtrak carried 31 million passengers across the continental United States and Canada, and operated more than 300 trains daily. Additionally, Amtrak and other passenger rail carriers operate in an open infrastructure with multiple access points that make it impractical to subject all rail passengers to the type of security screening that passengers undergo at airports. Notwithstanding this, there were actions that TSA could have taken, but did not, that would have strengthened rail security. Specifically, although required to by the *9/11 Act*, TSA neither identified high-risk carriers nor issued regulations requiring those carriers to conduct vulnerability assessments and implement DHS-approved security plans. TSA also did not issue regulations that would require a railroad security training program and security background checks for frontline employees. Regulations to implement a training program are important to ensure rail carriers have a mechanism in place to prepare rail employees for potential security threats.

Furthermore, unlike aviation and maritime port workers, TSA did not develop regulations requiring security background checks for rail workers. TSA vets airport and maritime port workers who need unescorted access to secure areas against the terrorist watchlist and immigration status and criminal history information, and these processes are consistent with the requirements in the *9/11 Act*.

[5] Public Law 110-53.

These very issues were identified in 2009 by GAO, which reported that TSA had only completed one of the key passenger rail requirements from the *9/11 Act*. Seven years later, we identified that the same rail requirements — a regulation for rail carriers to complete security assessments, a regulation for rail security training, and a program for conducting background checks on rail employees — remain incomplete.

Following the 2004 terrorist attack on a passenger train in Madrid, Spain, TSA issued a security directive for Amtrak. That directive required carriers to improve security procedures by designating a rail security coordinator, reporting significant security concerns to TSA, and allowing TSA to conduct inspections for any potential security threats. TSA does conduct some limited inspections to verify carrier compliance with these requirements. However, TSA does not enforce other aspects of the security directive, such as the use of bomb-resistant trash receptacles, canine teams, rail car inspections, and passenger identification checks to enhance security and deter terrorist attacks. Instead, TSA relies on Amtrak and other transit entities to implement security measures if resources permit, and is even considering rescinding these minimal requirements from the directive. Without enforcing all security requirements, TSA diminishes the directives importance and carriers ability to prevent or deter acts of terrorism.

Since the issuance of our report in May 2016, TSA has taken steps to implement two of the three remaining requirements. TSA issued a Notice of Proposed Rulemaking requiring security training for employees of higher-risk and anticipates a final rule by the end of the fiscal year. In the spring of 2018 TSA plans to issue a Notice of Proposed Rulemaking requiring security vetting for certain rail employees. TSA asserts that Executive Order 13771 (which establishes a requirement where an agency must eliminate two existing regulations for any new regulation the agency wishes to issue), is complicating the issuance of the agency's new rulemakings. If TSA does not fulfill these requirements, it cannot ensure that passenger rail carriers will implement security measures that may prevent or deter acts of terrorism.

Pending Legislation

Many of the issues I've discussed today are addressed in the S. 763, *Surface and Maritime Transportation Security Act*. I want to thank the Committee for introducing legislation to address a number of the challenges facing the Department. We believe that if enacted, this legislation will direct numerous improvements to our Nation's security. However, I must emphasize that the Department and TSA have demonstrated a pattern of being dismissive and lax on implementing requirements related to non-aviation security. Under these

circumstances, change will require significant attention by Congress, the Inspector General, and the Comptroller General to ensure that TSA and the Department take timely actions to implement these improvements.

Future work

We will continue to audit and evaluate the Department's aviation and non-aviation-related programs, report our results, and closely track report recommendations. Currently, we are reviewing the effectiveness of access controls to secured airport areas; Federal Air Marshal Service international flight operations and ground-based assignments; TSA's efforts to hire, train, and retrain its employees; and TSA's use of the Sensitive Security Information designation. We are also planning reviews on the security of rail facilities; TSA's canine program; and a review of TWIC that is mandated by P.L. 114-244, *Essential Transportation Worker Identification Credential Assessment Act*.

Madame Chairman, this concludes my testimony. I welcome any questions you or any other members of the Subcommittee may have.