

**Statement of David P. Pecoske**  
**Administrator**  
**Transportation Security Administration**  
**U.S. Department of Homeland Security**  
**before the**  
**United States House of Representatives**  
**Committee on Oversight and Reform**  
**“Identifying, Resolving, and Preventing Vulnerabilities in TSA’s Security Operations”**  
**June 25, 2019**

Good morning Chairman Cummings, Ranking Member Jordan, and distinguished members of the committee. Thank you for inviting me here today to testify about the Transportation Security Administration (TSA) and the work we are doing to keep our transportation system secure. I am grateful for the constructive relationship TSA enjoys with Congress, the Department of Homeland Security Office of Inspector General (DHS OIG), and the Government Accountability Office (GAO). We all share the same goal of keeping travelers secure, on behalf of all the men and women of TSA, we appreciate the continued support of this Committee, as we carry out our vital security mission.

As I mentioned when I testified before this committee last year, TSA strives to remain a learning organization – one that continuously assesses and proactively improves all aspects of how the agency performs its mission. Through our own internal testing processes as well as feedback the agency receives through external oversight, TSA continues to learn, evolve, and improve its people, processes, and technology to better meet present and future threats and challenges.

The U.S. commercial aviation system accommodates approximately 965 million domestic and international aviation passengers annually – this equates to the screening of 2.2 million passengers, 1.4 million checked bags, and 5.1 million carry-on bags each day. As aviation transportation remains a highly-valued target for terrorists, and terrorist modes and methods of attack are more decentralized and opportunistic than ever before, TSA is challenged each day by a constantly evolving threat environment, both in the physical and cyber realms. Compounding the challenge, TSA has managed the nearly four percent annual passenger growth experienced over the last few years with only modest increases in the size of its Transportation Security Officer workforce. In fact, TSA is preparing for its busiest summer ever, with anticipated checkpoint volume growth of nearly 4.7 percent across the board compared to last summer. From Memorial Day through Labor Day, TSA expects to screen more than 262 million passengers and crew.

Similarly, TSA sees increased volume in air cargo – expecting an increase of 2.5 percent this year – and continuing expansion in the surface transportation arena, where over 5.3 billion passengers travel on transit and over-the-road buses each year; more than 10.1 billion passenger trips on mass transit per year; and nearly 900,000 chemical shipments on trucks every day. Beyond those usage numbers associated with a relatively open network of transportation modes, the physical scope of the system encompasses approximately 126,000 miles of railroad tracks; 4.2 million miles of highway; 615,000 highway bridges; 473 road tunnels; and nearly 2.5 million miles of pipeline.

As requirements on our transportation system increase, we must always remember that we face ambitious adversaries on a daily basis – ones who watch us, study our vulnerabilities, and work diligently to develop new attack strategies to replace those that have failed.

Consequently, TSA must remain vigilant in continually assessing vulnerabilities, identifying threats, and mitigating risks to ensure passengers and commodities move through the aviation transportation system securely and efficiently. To that end, TSA uses the observations gained through DHS OIG covert testing, GAO's assessment of TSA's covert testing process, and our own internal assessments to both understand vulnerabilities and the root causes and then to take corrective actions to improve the people, processes, and technology employed to ensure the security of the transportation system.

TSA established the Security Vulnerability Management Process (SVMP) to assist with the management of security vulnerabilities identified by external and internal sources as well as the tracking of TSA's mitigation efforts. Through this process, TSA formally established an analytic framework for submitting, evaluating, and tracking the mitigation of vulnerabilities. At my direction, the agency recently strengthened this process further in response to a GAO recommendation. These changes will improve the agency's ability to address security concerns across the enterprise, prioritize and allocate resources to address numerous threats, and apply strategic planning and risk-informed decision-making.

Last year, TSA issued its 2018-2026 TSA Strategy and Administrator's Intent, which is being used as an implementation tool for key TSA initiatives, including several that seek to improve security and TSO performance at the checkpoint. Through these actions and activities along with the work being done through our Inspections and SVMP processes, TSA is working diligently to address the recommendations from the DHS OIG's 2017 and recent GAO covert testing audits. The TSA Strategy establishes three key priorities for the agency: improve security and safeguard the transportation system, accelerate action, and commit to our people. These strategic priorities reflect TSA's need to improve performance through reassessing the

effectiveness of our procedures, personnel, and technology. To that end, TSA accelerated its procurement of more effective and technically capable checkpoint screening equipment (e.g., Computed Tomography and Credential Authentication Technology units); invested in enhancing the training and retention of our frontline personnel through the TSO Career Progression Program, which seeks to reward officers for attainment of advanced training and skills; and revised screening procedures to improve detection capabilities. All of these efforts were informed by lessons learned through external oversight and internal inspections.

Covert testing remains a critical tool for TSA to evaluate and understand its security effectiveness. TSA appreciates GAO's recommendations on ways the agency can improve our internal testing programs to better secure the traveling public. Informed by GAO's observations, I consolidated TSA's covert testing programs and directed a new covert testing effort to regularly assess the effectiveness of checkpoint screening over time – referred to as Index testing. This long term testing program will give TSA an invaluable tool to measure the effectiveness of people, process, and technology against adversary-based threat scenarios. Information generated from this testing will establish a security baseline with which we will be able to more rigorously assess and test vulnerabilities in our screening system. This more rigorous approach to vulnerability assessment afforded by Index testing will ensure we are implementing not only the most effective vulnerability mitigations, but also provide clarity on the return on our security dollars.

Index testing will be conducted with a mixture of personnel, many of whom have volunteered and been trained to serve as part-time testing “reservists.” This “Red Team Reserve” corps is cost effective and provides our headquarters personnel with a unique appreciation of the challenges faced by our front-line workforce and an in-depth understanding

of TSA's core-mission. All personnel involved in testing receive a mixture of classroom and in-the-field training to support testing consistency – an issue identified by GAO in airport-based testing.

In response to the GAO's recommendations, TSA is developing a program to assist Federal Security Directors (FSDs) in improving their respective local covert testing programs. The data collected will be used to enhance program implementation, share beneficial practices, and improve the covertness, consistency and data analysis of all local covert testing. These efforts will ensure that FSDs can collect data about their airport's performance and can use testing locally to improve their airport's overall security effectiveness.

Many of the challenges our agency faces do not have one-off solutions, and require an iterative and collaborative process to reach the goal we all share of closing known vulnerabilities. Rest assured, I will continue to work closely with the DHS OIG, and the GAO, and rely on their keen insights, to assist the agency in its continued development of solutions to the challenges we face. I know I can speak for all of us in this room, that our shared priority will always be keeping the traveling public safe and secure. On behalf of all the men and women of TSA, I would like to thank Chairman Cummings and Ranking Member Jordan, and all the members of this Committee for your continued support, and I look forward to your questions.