Statement of Dr. Huban A. Gowadia

Acting Administrator

Transportation Security Administration

U.S. Department of Homeland Security

before the

U.S. House of Representatives

Committee on Oversight and Government Reform

March 2, 2017

Good morning, Chairman Chaffetz, Ranking Member Cummings, and distinguished Members of the Committee. Thank you for the opportunity to appear before you today to discuss the Transportation Security Administration's (TSA) approach to information security as we execute our mission to protect the Nation's transportation systems. I appreciate the Committee's interest in ensuring TSA operates transparently, collaborates, and shares information with its partners and stakeholders, and appropriately protects against the release of sensitive information which could cause harm in the hands of our adversaries.

TSA's mission is to protect the nation's transportation systems to ensure freedom of movement for people and commerce. Our agency faces a persistent and evolving threat from terrorist groups around the world, exacerbated by homegrown violent extremists inspired by messages of hatred to do harm to the American people. To mitigate this threat, TSA works collaboratively with a wide range of partners, from aviation and surface transportation industry stakeholders and international counterparts to intelligence and law enforcement community professionals. On the frontlines, more than 44,000 Transportation Security Officers screen over

2 million passengers, 1.3 million checked items, and 4.9 million carry-on items at more than 430 airports every day. More than 700 Transportation Security Inspectors ensure regulatory compliance, and more than 900 canine teams support security missions, while Federal Air Marshals (FAMs) last year flew more than a billion miles on international and domestic flights, including thousands of special mission coverage flights, providing professional counterterrorism law enforcement protection to the nation. TSA's Visible Intermodal Prevention and Response teams collaborated with more than 750 law enforcement and transportation stakeholder organizations nationwide to conduct more than 8,500 operations at hundreds of locations across all modes of transportation. TSA also inspects nearly 300 international airports with direct flights into the United States, regulates foreign and domestic repair stations, and works with its surface stakeholders to secure roadways, railroad tracks, bridges, tunnels, pipelines, and transit systems. Successfully securing the Nation's transportation system in a challenging, dynamic threat environment requires constant communication with a variety of audiences. We must communicate reliable information with the travelling public, provide intelligence and operational information to TSA's workforce in the field, and foster close collaboration with our transportation security partners.

Information Sharing with Transportation Security Partners

TSA participates actively in a number of collaborative organizations at local, national, and international levels to share information with transportation security partners, develop policy recommendations, and solicit feedback. As codified by the *Aviation Security Stakeholder Participation Act of 2014* (Public Law 113-238), TSA has established the Aviation Security Advisory Committee (ASAC), comprising representatives of air carriers, airport operators, labor

organizations, security technology companies, law enforcement and security experts, as well as many other important stakeholders. The ASAC holds regular meetings and advises TSA on the development, refinement, and implementation of policies, programs, rulemaking, and security directives pertaining to aviation security, including through established subcommittees pertaining to specific aviation security issues. From the current two-year term ending in April 2017, ASAC presented 45 recommendations, of which 33 are complete and 12 are in the process of being implemented.

In the surface mode, TSA consults with stakeholders through Sector and Government Coordinating Councils, as well as through the DHS-led Critical Infrastructure Partnership Advisory Council (CIPAC) and other industry-centric organizations such as the Mass Transit Policing and Security Peer Advisory Group. TSA also works closely with our counterparts at the Department of Transportation to integrate safety and security priorities.

Internationally, in coordination with the Department of State, TSA Representatives and International Industry Representatives stationed overseas liaise with foreign governments and airport stakeholders and facilitate coordination with foreign and domestic air carriers overseas. Additionally, TSA is a leader in a number of regional and international organizations concerned with transportation security, such as the International Civil Aviation Organization and the Quadrilateral Working Group. TSA also partners with key industry trade associations such as the International Air Transport Association to help drive industry security policy and critical aviation issues.

Further, TSA conducts outreach with civil rights, disability-related, and multicultural interest groups to understand concerns and solicit feedback on TSA's policies and programs. Groups such as the Sikh Coalition, the National Center for Transgender Equality, the American

Diabetes Association, and the Helen Keller School for the Blind participate in TSA's Disability and Multicultural Coalitions and have partnered with TSA to provide training for the workforce. TSA communicates openly with the public and press via public outreach, websites, social media, and media relations. TSA conducts more than 300 media events per year and responds to approximately 10,000 media inquiries, and TSA operates the AskTSA program to answer customer questions and provide helpful services in real-time 365 days a year via Twitter and Facebook Messenger platforms.

Taken together, TSA's engagement efforts provide avenues for daily interaction and information sharing with stakeholders of all varieties, including the sharing of classified intelligence products and Sensitive Security Information (SSI) as appropriate.

Over the past year, TSA has increased our efforts to communicate and collaborate with industry stakeholders, resulting in significant improvements to our security operations. Partnership with airports and air carriers was crucial to addressing large passenger volumes last spring and summer, as industry partners across the country assisted TSA by carrying out functions such as: enforcing 1+1 carry-on baggage regulations, providing staffing support to conduct non-security related duties, providing volume projections to inform staffing, promoting TSA Pre✓®, and reminding passengers to arrive early. TSA established an Airport Operations Center (AOC) at TSA Headquarters, which holds daily calls with industry partners to ensure clear, timely communication. Using nationally-accepted incident management concepts, the AOC continues to closely track daily screening operations and shift officers, canine resources, the National Deployment Force, and other security resources to meet mission demands in advance of predicted passenger volume.

Last year, we also deployed a team of TSA experts in staffing, scheduling, and screening operations to partner with industry at the 21 largest airports for optimization insights. During these visits, TSA worked closely with air carrier and airport industry partners to review airline schedules, passenger volumes, and queue design, as well as checkpoint and baggage screening areas for improvement opportunities. These visits produced an action plan for each airport's Federal Security Director (FSD) to implement prior to the summer travel season. Fulfilling a mandate of the *FAA Extension, Safety, and Security Act of 2016* (Public Law 114-190), TSA has built on this model to establish quarterly stakeholder meetings at each airport through which FSDs engage on a regular basis with stakeholders to exchange information regarding airport security operations. These efforts have improved our ability to deploy the resources we have in the most efficient and effective manner possible to screen the record numbers of passengers transiting through our Nation's airports.

Sensitive Security Information (SSI)

Given TSA's need to share information with a wide range of security partners and stakeholders, we take seriously our responsibility to protect information that, if publically released, would be detrimental to transportation security. TSA works to ensure that sensitive information is properly marked, handled, and distributed in accordance with the SSI regulation to protect this information from unauthorized disclosure. TSA also recognizes the need for transparency and public access to information not deemed security sensitive.

Sensitive Security Information, or SSI, is one of the few types of sensitive but unclassified information required by statute. Congress authorized the Federal Aviation Administration to designate SSI in the 1970s, and the FAA promulgated regulations to

implement the congressional mandate. When TSA was created, Congress also authorized TSA to designate information as SSI, as codified at 49 U.S.C. § 114(r). TSA regulations promulgated to implement this mandate are found at 49 C.F.R. Part 1520. When it provided TSA with SSI designation authority, Congress also empowered the Administrator of TSA to make final determinations regarding SSI.

Within DHS and TSA, the SSI Program Office is charged with the day-to-day management, consistent application, identification, safeguarding, and redaction of SSI. Housed within the Office of Law Enforcement/Federal Air Marshal Service, which is charged with managing TSA's classified information program, the SSI Program Office is staffed by career professionals with significant experience and a comprehensive understanding of SSI and its role in transportation security. The SSI Program Office works closely with subject matter experts throughout TSA to understand and identify information that could be used by our adversaries to carry out attacks on the transportation network.

The DHS and TSA Management Directives (MDs) and associated guidance, which govern the SSI Program, provide direction for ensuring that SSI is treated in a manner consistent with the SSI statute and regulation. These directives require the release of as much information as possible without compromising transportation security, while taking into consideration the information's operational use to adversaries, level of detail, the public availability of the information, and the age of the record. TSA's goal is to redact as little information as possible while still protecting the SSI.

Over the past several years, TSA has significantly enhanced the SSI Program's policies, training, and management of SSI. TSA has updated SSI training and mandated it for all TSA employees and contractors on an annual basis; refined the redaction process; developed a

comprehensive Policies and Procedures Handbook to eliminate gaps in previous guidance; defined specific roles and responsibilities for the safeguarding of SSI; improved reference guides for DHS employees and contractors; leveraged available technologies to improve operations; and, per a recommendation from this Committee, standardized the process through which the Administrator may revoke the SSI designation for specific information.

We recognize that effective training is integral to our management of the SSI Program. Annual SSI training required of all TSA personnel includes reviewing principles of identifying, marking, safeguarding, disclosing, and destroying SSI. Additionally, every TSA office and field location is required to maintain at least two persons who have completed the Advanced SSI Training and Certification Course. These individuals have participated in detailed SSI training, passed the SSI Certification Examination, and continue to maintain a high level of proficiency through annual participation in Continuing Education in SSI. In accordance with DHS and TSA MDs, this SSI Coordinator network is required to complete an annual self-inspection to validate program compliance. The SSI Program Office has also conducted targeted SSI advanced training and awareness activities for key TSA stakeholders, DHS components, and other federal agencies.

In 2015, TSA updated the *SSI Policies & Procedures Handbook*, which provides a single, comprehensive resource for personnel to consult regarding their responsibilities concerning SSI. The Handbook replaced a previously issued series of discrete, independent, and less detailed SSI policies. It was extensively coordinated, provides guidance and assistance in a user friendly format organized by subject matter, and covers SSI topics including identifying, marking, safeguarding, disclosing and destroying SSI, along with overviews of SSI training and awareness of programs and instructions for the reporting and adjudication of SSI that is lost, stolen, or

subject to unauthorized disclosure. The Handbook is readily available to all TSA personnel on the TSA intranet, increasing TSA's ability to ensure consistency in SSI designations and protections.

In addition to all of these recent efforts to improve TSA's stewardship of SSI, there are well established DHS and TSA procedures to address challenges to SSI designations. These processes are regularly deployed when, for example, the Government Accountability Office and the DHS Office of Inspector General conduct oversight, draft reports of their findings, and submit those draft reports to TSA for sensitivity reviews. We encourage the use of these procedures to resolve reasonable differences of opinion and maximize transparency, while also protecting sensitive information developed by TSA and our security partners from falling into the hands of those who would do us harm.

TSA understands the importance of the SSI designation while recognizing the value of transparency and the need for the public to have access to as much information as possible. We will continue to seek out opportunities to further improve how SSI is identified, managed, redacted, and safeguarded.

Collaboration with the Government Accountability Office (GAO), the DHS Office of Inspector General (OIG), and the U.S. Office of Special Counsel (OSC)

TSA appreciates the value of the audit and investigative work accomplished by the Government Accountability Office (GAO), the DHS Office of Inspector General (OIG), and the U.S. Office of Special Counsel (OSC). We endeavor to provide GAO, OIG, and OSC experts with information they require in a timely and comprehensive manner and with appropriate markings and classifications.

As the Committee is aware, the OIG is in the midst of an inspection of TSA's SSI Program, policies, and processes, and we look forward to receiving and reviewing their recommendations. In the meantime, we continue to cooperate with all OIG audits, inspections, and investigations and implement recommendations from past reports.

TSA also provides information upon request to the OSC regarding whistleblower retaliation complaints and other applicable prohibited personnel practice allegations, and we value their endeavors to bring to light any instances of impropriety against our employees. Under my leadership, TSA will not tolerate retaliation against whistleblowers, and we will continue to encourage employees to voice their views through a variety of available tools and services and to provide opportunities for redress and due process. I strongly support and encourage employees to disclose any perceived violations of law, rule, or regulation, gross mismanagement or waste of funds, abuse of authority, or substantial and specific danger to public health or safety to the DHS OIG, the U.S. Office of Special Counsel, or any other appropriate person or entity.

Conclusion

TSA is tasked with a complex, critical security mission that can only be accomplished through close collaboration with stakeholders and partners. We attempt to share information as openly as possible while accounting for the constantly evolving threat posed by enemies who wish to do us harm. We will continue to develop and refine our practices to ensure we meet the highest standards of transparency possible. Thank you for the opportunity to appear before you today and for the Committee's support of TSA's important mission.

Acting Administrator

Huban Gowadia

Huban Gowadia is the Deputy Administrator of the Transportation Security Administration. In addition to guiding implementation of the Administrator's strategic goals, she oversees the day-to-day operations of TSA. As a proven counterterrorism and security professional, she provides leadership, direction and guidance to further the Administrator's goals for the agency and assists in determining TSA policies, objectives and priorities.

Dr. Gowadia's career is rooted in strategic, operational, and interagency experience in homeland security.

Prior to joining TSA, she most recently served as Director of the Domestic Nuclear Detection Office at the U.S. Department of Homeland Security where she led DHS's coordinated efforts to protect the United States from nuclear attack. Under her direction, DHS advanced national nuclear forensics capabilities and coordinated government-wide efforts to enhance worldwide capabilities to detect, analyze and report on nuclear and other radioactive materials that are out of regulatory control.

She also served as Program Executive for DHS's Science & Technology Directorate, where she led the Countermeasures Test Bed, evaluating next-generation technologies for detecting explosives and nuclear materials, operational requirements and response protocols.

Dr. Gowadia began her federal career with the Federal Aviation Administration in 2000, working on aviation security technologies and policy. When the office transitioned to TSA as the Office of Security Technologies in 2001, she served as Checkpoint Program Manager and after September 11, 2001, she led TSA's initiative to replace all walk-through metal detectors at airports with enhanced systems.

Dr. Gowadia received a Bachelor of Science degree in Aerospace Engineering from the University of Alabama and a Doctorate of Philosophy in Mechanical Engineering from Pennsylvania State University.