INSIDER THREATS TO AVIATION SECURITY: AIRLINE AND AIRPORT PERSPECTIVES

STATEMENT OF LAUREN BEYER
VICE PRESIDENT, SECURITY AND FACILITATION, AIRLINES FOR AMERICA
BEFORE THE
UNITED STATES HOUSE HOMELAND SECURITY COMMITTEE
TRANSPORTATION AND PROTECTIVE SECURITY SUBCOMMITTEE

SEPTEMBER 27, 2018

Good morning Chairman Katko, Ranking Member Watson-Coleman, and members of the Subcommittee. My name is Lauren Beyer, and I am the Vice President for Security and Facilitation at Airlines for America (A4A). Thank you for inviting me here today to discuss insider threats to aviation security.

Overview. The safety and security of our passengers and employees is our single highest priority. We take aviation security very seriously. We share this common goal with the Transportation Security Administration (TSA) and work cooperatively and collaboratively with them every day to keep our skies safe and secure.

When talking about the daily challenges of aviation security it is important to understand the depth and magnitude of what takes place and what is transported by air every single day. On a daily basis, U.S. airlines ---

- Fly 2.3 million passengers worldwide;
- Carry more than 55,000 tons of cargo;
- Operate approximately 27,000 flights;
- Serve more than 800 airports in nearly 80 countries; and
- Directly employ more than 715,000 (full-time and part-time) workers across the globe.

Given the vast geography and sheer volume of air travel it is exceedingly important that we approach security in a smart, effective, and efficient manner that best utilizes the finite resources available in a system that both improves security and facilitates commerce. This becomes even more imperative given the expectation that both passenger and cargo traffic are expected to grow in the coming years. As an industry, we believe that system is best represented through the principles of risk-based security – which is the lynchpin and bedrock of our security system today.

Risk-Based Security. The administration of risk-based security principles is of paramount importance to aviation security. A risk-based approach recognizes that “one size fits all” security is not the optimum response to threats, including from insiders. Risk-based, intelligence-driven analysis has been a widely accepted approach to aviation security for some time. We know the effectiveness of risk-based security and we therefore strongly support it.

One of our nation's greatest challenges is to strike the right balance between managing risk and over-reaction. Enhanced mitigation of insider threats and the efficient operation of our nation's airports are not mutually exclusive goals; government and industry must continue to work together to find pragmatic approaches that appropriately balance these issues. By utilizing and following risk-based principles we provide a security framework that can be nimbler and more responsive to current and emerging threats and allows TSA and industry to focus finite resources on the highest risks. This framework also takes the operational complexity of the U.S. aviation system into account.

Insider Threats. Insider threat—individuals with privileged access to sensitive areas, equipment, or information who misuse this access and compromise security—is of great concern to the aviation industry.

That is why carriers have acted to address this risk. A sampling of measures includes:

- Enhancements to access control such as the use of biometrics and CCTV coverage;
- Implementing "see something, say something" campaigns or other challenge programs;
- Providing multiple avenues for reporting of suspicious activity – credited or anonymous – with incentives for such reporting; and
- Offering employee assistance programs addressing issues such as stress management, work-life balance, and grief and loss.

Incident at SEATAC. The tragic incident at Seattle-Tacoma International Airport in August of this year is a somber reminder of the constant vigilance required to keep our skies safe. These kinds of incidents require careful investigation and root cause analysis to determine corrective actions that may be required to mitigate identified security vulnerabilities. There is much at stake and it is critical authorities thoroughly investigate and analyze all facts.

The industry is not sitting idly by while the investigation is on-going, however. In fact, A4A along with many of our stakeholder partners has initiated an effort to bring together subject matter experts from across the industry and government to solicit and thoroughly evaluate airport and aircraft security best practices. These practices will be shared across the U.S. aviation industry. These best practices will also inform the work of the Aviation Security Advisory Committee (ASAC) Subcommittee on Insider Threat previously tasked by the TSA Administrator to review and make recommendations to address insider threat more broadly.

Aviation Security Advisory Committee. We strongly believe the ASAC, of which A4A is a member, is the appropriate venue in which to examine these matters and produce recommendations. The ASAC includes representatives from across the aviation industry and is the traditional mechanism through which TSA and industry collaborate to develop the most effective aviation security measures.

As this Subcommittee will remember, in 2015 the ASAC created a working group tasked with analyzing the adequacy of existing security measures and recommending additional measures to improve employee access controls. The effort was supported by the Homeland Security

Studies and Analysis Institute (HSSAI), which provided independent and objective subject matter expertise, as well as by representatives of TSA. That effort produced 28 recommendations for effective measures to protect against possible acts of criminality and terrorism, measures that could be tailored to the unique environment at each airport. Airlines strongly supported and worked collaboratively with TSA, airports and other stakeholders to implement the ASAC recommendations. Three years later, we applaud TSA and the larger aviation community for implementing the vast majority of these recommendations and continue to urge full implementation of those that are still pending. While our work is obviously never done, the guideposts provided by the ASAC recommendations have and will continue to play an important role in improving our risk-based system.

Access Control. One aspect of access control that has received much attention over the last several years is security screening and inspection of employees, and deservedly so. We continue to believe that physical screening of employees is one of several elements that should be used in combination to enhance access control. We applaud the Subcommittee, and Chairman Katko in particular, for his efforts to initiate a cost and feasibility study to assess the impact of employee screening which would include a comparison of estimated costs and effectiveness to the federal government, airports, and airlines. We believe that analysis will be critical in establishing how best to move forward and improve access control procedures.

We are also strong supporters of multiple security layers deployed on a risk-based and unpredictable basis. Indeed, the International Civil Aviation Organization (ICAO) recommends increased use of random and unpredictable security measures to contribute to deterrence and to increase mitigation against the potential tactical advantage of insiders. This potential advantage is precisely why flexibility and agility rather than static or predictable processes are key to guard against insider threats. We believe that random and unpredictable checks should be conducted at a frequency significant enough to provide employees with a reasonable expectation that they will be subjected to such checks at any point during their work. That is why we supported the employee screening improvements enacted by Congress in 2016 as part of the Federal Aviation Administration, Safety and Security Act of 2016 (P.L. 114-190), which directed TSA to expand the use of Transportation Security Officers to conduct random physical inspections of airport workers in a risk-based manner. TSA leverages its Advanced Threat Local Allocation Strategy (ATLAS) aviation worker screening program to allocate resources for these random inspections, and we support further expansion of the program.

As mentioned, we believe physical screening is only one of several necessary elements to ensure effective access control. Other critical elements include enhanced and perpetual vetting, security awareness training, and intelligence and information sharing. We continue to urge TSA to expand the list of disqualifying crimes for those seeking a Secure Identification Display Area (SIDA) badge as well as to align the list of disqualifying offenses with other government programs, particularly those of U.S. Customs and Border Protection (CBP). We also urge TSA to extend the lookback period for criminal history records checks.

Stop the annual practice of diverting passenger security fee revenue. U.S. aviation and its customers are subject to 17 federal aviation taxes and 'fees'. Included within those numbers are revenues that are intended to support activities within the TSA, including the September 11th TSA Passenger Security Fee. As this Subcommittee knows well, that 'fee' is $5.60 imposed per one-way trip on passengers enplaning at U.S. airports with a limit of $11.20 per round trip; the fee also applies to inbound international passengers making a U.S. connection. However, starting in Fiscal Year 2014, Congress started diverting a portion of that fee toward general deficit reduction and is scheduled to continue diverting these critical resources through Fiscal Year 2027. From our perspective, this policy is simply unacceptable. Airlines and their customers now pay $1.6 billion more in TSA security fees —$3.9 billion (2017) vs. $2.3 billion (2013)—for the exact same service. The concept of a 'fee' specifically charged to pay for a specific service has long been lost in our industry and they have all simply become taxes by another name. We would respectfully request this Committee do everything in its power to redirect TSA passenger security fee revenue back where it belongs: paying for aviation security. These diverted funds could go a long way to increase TSA capacity to mitigate insider threats, including increased TSA risk-based, unpredictable physical inspections of airport workers at secure area access points and within the secure area.

We appreciate Congressman DeFazio and Senator Markey's leadership on this issue through introduction of legislation to eliminate the diversion of security fees.

Importance of Commercial Aviation Sector. Airlines crisscross the country and globe every day carrying passengers and cargo safely and securely to their destinations, and this is an integral part of the economy. In 2014, according to the Federal Aviation Administration (FAA), economic activity in the U.S. attributed to commercial aviation-related goods and services totaled $1.54 trillion, generating 10.2 million jobs with $427 billion in earnings. As of December 2016, our industry contributes 5% of our nation's GDP. These figures, while both impressive and important, fail to consider the incalculable value of the passengers and crew flying on commercial flights every day. These facts underscore what is at stake and why we need to approach aviation security in a smart, effective, and efficient manner to make sure we get it right. The daily collaboration and communication between TSA and stakeholders will play a vital role toward increasing system-wide protection and lowering risk without unnecessarily clogging up the system.

Thank you, on behalf of our member companies, we appreciate the opportunity to testify.