Statement of Wendy Reiter, Director, Airport Security, Port of Seattle

U.S. House of Representatives Homeland Security Committee

Subcommittee on Transportation and Protective Security

"Insider Threats to Aviation Security: Airline and Airport Perspectives"

September 27, 2018

Chairman Katko, Ranking Member Watson Coleman and members of the Committee, thank you for the opportunity to discuss aviation insider threat and perimeter security issues with you today. My name is Wendy Reiter, and I currently serve as the Director of Aviation Security for Seattle-Tacoma International Airport (Sea-Tac), which is owned and operated by the Port of Seattle. I also recently served as Vice-Chair of the Transportation Security Services Committee of the American Association of Airport Executives.

Sea-Tac Airport has long prioritized the safety and security of our passengers, employees and nearby residents as our top responsibility. As an independent port authority governed by directly elected Commissioners, protecting against threats both external and internal is a core part of our DNA. This commitment has driven Sea-Tac to do everything reasonable to invest in infrastructure, technology and procedures that increase aviation security – above and beyond what is required of us by federal law – which has made us one of the leading airports in the country as it relates to insider threat and perimeter security.

We deeply appreciate the partnership we have with the Transportation Security Administration (TSA), including both local TSA staff as well as TSA leadership in Washington, DC. I also want to thank the Subcommittee for your work on the Checkpoint Optimization and Efficiency Act, which has resulted improved collaboration, communication and information sharing at the local level.

I am pleased to be here today to share some of the specific tactics we have employed at Sea-Tac, although I will note that we are not here to suggest that all airports should adopt these exact practices. As the old saying goes, "if you've seen one airport, you've seen one airport," and so we recognize that it is up to each airport's local leadership to determine how to best invest limited resources for maximum return. This is particularly true for insider threat issues, which may not be fully preventable no matter how many layers of security and redundancies are put into place.

Let me start with our approach to insider threat, which is mainly focused around three key aspects: credentialing, biometrics, and physical employee screening. First, in terms of credentialing, we work closely with the Transportation Security Administration (TSA) and Federal Bureau of Investigation (FBI) to conduct regular background checks on all employees, both scheduled and unscheduled. Those badges not only allow us to ensure that sterile areas are restricted to vetted employees but also to use access controls to further limit specific areas of the airport and airfield to only the most relevant employees. We are also planning by the end of this year to be enrolled in the"Rap Back" program to ensure that badge

access is immediately revoked from anyone with a newly discovered disqualifying crime.

Second, each of our sterile-area access doors requires both a badge scan and a biometric fingerprint scan. The biometric element has been in place at Sea-Tac since shortly after September 11, 2001, and is an additional layer of security that allows us to confirm that the badge matches the user. In certain cases, we have added a third level of authentication to require the user to scan and swipe their badge as well as enter a uniquely-assigned personal identification number (PIN).

Third, as of spring 2017, we have implemented physical screening for all employees accessing the sterile areas of the airport terminals. We have multiple checkpoints, each with a magnetometer, that are staffed by Port of Seattle employees hired specifically for this purpose. Full employee screening required a significant upfront investment and major recurring costs to the airport, but we have been very pleased with the results in terms of both security and employee convenience. We've been able to process as many as three hundred employees per hour, and have now screened approximately 1.5 million individuals over the last year and a half. This screening has resulted several times in the seizure of both weapons and drugs, which we believe we would have been not caught without such a system in place.

At Sea-Tac, we have 500 different employers operating at the airport, and there are limitations to the requirements that we can impose on all of those different entities and their workers. We rely on a partnership ethic to make any substantive

changes to protocols and practices, and we are grateful for their openness to pursuing these important investments.

As it relates to perimeter security, Sea-Tac has made major investments in both employee screening and explosive detection canines.While we've had physical screening of employees inside the airport for the last year and a half, our plan is to institute the same level of security at all of our airfield perimeter gates by the middle of 2019. This new procedure will require every person entering the airfield to walk through a magnetometer, and will include visual screening of all vehicles – again by specifically trained Port of Seattle staff.

We have also invested in purchasing our own explosive detection canines. In addition to the eight Port of Seattle Police Department canine teams trained at the TSA canine training center at Lackland Air Force Base to sniff stationary objects for explosives, the Port two years ago purchased three Air Scent-trained dogs from K2 Solutions in North Carolina. These dogs are trained to detect and trail explosive odors on a moving person, which is a huge advantage in the front of the airport around ticketing and baggage claim. The Port Police are the first law enforcement agency in Washington state to have certified working Air Scent Teams.

At the end of the day, all security systems are based on thoughtful risk management and maximizing the use of resources that can have the biggest impact. No security system is perfect or able to anticipate every potential action, and we need to continue to adapt security protocols to meet new challenges.

Sea-Tac is a perfect example of this truth: despite all of the measures I just listed, we still experienced a high-profile insider incident just last month.

The need to remain vigilant and constantly improve is why Sea-Tac recently joined in creating a new Industry Working Group on Aviation Security Best Practices. Last month, aviation industry representatives from Airlines for America, Airports Council International-North America, the American Association of Airport Executives, the Cargo Airline Association, the Regional Airline Association, and the National Air Carrier Association met to discuss how we can collectively baseline aviation industry best practices. The group agreed that the best practices identified through this working group should be shared with the U.S. aviation industry, and should also inform the work of the TSA's Aviation Security Advisory Committee's (ASAC) Insider Threat Subcommittee. The ASAC subcommittee has committed to incorporating these recommendations into its final report.

As part of the working group's efforts, we are in the process of surveying aviation industry peers about best practices, and hope to have recommendations by the end of this year. Specific topics for investigation include aircraft security, employee training and reward programs, mental health programs, and airport coordination/operation centers. Sea-Tac has also intitiated an independent third party after-action report of our most recent insider incident, which will contain recommendations for changes that our airport will consider.

I want to close by noting this confluence of activities that are coming together toward the end of the year. In his testimony to the Senate Commerce Committee

earlier this month, TSA Administrator David Pekoske shared that he expects ASAC to report back to him by the end of the year on the status of their insider threat recommendations. Combined with the Sea-Tac after-action report, potential TSA and FBI reports on the recent Sea-Tac incident, and the industry working group findings, the aviation community will have an incredible opportunity in early 2019 to thoughtfully discuss opportunities to move forward in impactful ways on insider threat. I look forward to working with this committee and others at that time.

Thank you for your time today, and I welcome any questions you may have.