Testimony of Kathleen M. Carroll

Vice President, Government Affairs

HID Global

on behalf of the Security Industry Association (SIA)

before the

United States House of Representatives

Committee on Oversight and Government Reform

Subcommittee on Transportation and Public Assets

Securing Our Skies: Oversight of Aviation Credentials

February 3, 2016

Good afternoon Chairman Mica, Ranking Member Duckworth and distinguished Members of the Committee. Thank you for the opportunity to appear before you today to discuss how private industry can contribute to and support all stakeholders in securing our Nation's airports.

I am testifying on behalf of the Security Industry Association (SIA), a non-profit international trade association representing more than 600 companies that develop, manufacture and integrate electronic and physical security solutions. SIA member companies provide security solutions to the Department of Homeland Security and its components to help protect critical infrastructure, including chemical facilities, seaports, mass transit systems, government facilities, and the nation's airports. I am the Chair of SIA's Government Relations Committee and I also chair the Privacy and Public Policy Committee for the International Biometrics and Identification Association (IBIA).

The Security Industry Association's member companies recognize that TSA has built a multi-layered security system that is risk-based. It is our belief that to confront ever-evolving threats to aviation security, all stakeholders – airlines, airports, vendors, and government agencies – should be working more closely with private industry. We believe that if we work closely with all stakeholders, we can increase security exponentially.

We also recognize that TSA has been working diligently towards solutions that further enhance security in the nation's 440 airports. To that end, TSA requested that the Aviation Security Advisory Council (ASAC) analyze the adequacy of existing security measures and recommend additional measures to improve employee access controls.

For purposes of my testimony today, I am going to address those areas where SIA and its member companies are already providing security solutions that will help the TSA and all stakeholders better secure our nation's airports and ensure the safety of the traveling public.

The ASAC identified five areas of analysis and generated 28 recommendations where TSA and the airline industry can take action to address potential vulnerabilities. I will focus on just a few. First, I will comment on the recommendation for biometric confirmation of identity for badge issuance and random auditing capture of a biometric template of SIDA (a security identification display area badge) applicants.

Biometrics are already in use at several airports, including BWI and SFO. These biometric deployments enhance security by tying the SIDA badge to the holder of the badge. Further, biometric technology has improved substantially in recent years and industry continues to invest in further advancements. There are several key measures to help ensure optimum performance of a biometric system that should be included in any standard that TSA establishes as recommended by the ASAC.

One is false acceptance rate or FAR which sets the level of security. Another is the false rejection rate which delivers a good customer experience. You can't have one without the other. Another key measure is liveness detection which eliminates spoofing. For example, liveness detection solves the worry around the biometrics that were stolen in the OPM breach. Biometrics information is worthless if it isn't usable. With liveness detection, the only way it is usable is if the living human being presents their biometrics. The bottom line: biometrics uniquely identifies airport employees in a consistent and secure manner.

Beyond biometrics, the security industry recommends that airport worker credentials follow a federated model. Why? And what is a federated credential? Many airport employees work at multiple airports and often need to go through the vetting process and carry a badge for each airport. In a federated model, such as the US Government's Personal Identity Verification (PIV) program, each federal employee is vetted to an acceptable and known process across all Federal agencies.

This multiple credentialing requires that employees who cross-credential carry a variety of documents with them all the time – passport, driver's license, even social security cards and/or birth certificates. There is a tremendous security risk in carrying all of this critical and sensitive documentation all the time.

PIV credentials use the Public Key Infrastructure (PKI) as one of several security features so that the credential can be trusted for access to all physical government buildings and all computer networks. In addition, the PIV credential is built on the Federal Information Processing Standard created by NIST. And, PKI allows for instant revocation of a credential across all these systems from a central location. This satisfies the requirement that badges be deactivated when a worker is terminated.

Airports are like the Federal government. Employees from different airlines fly to multiple airports several times a day. Airline and airport employees have access to sensitive, sterile areas within the airport. And while some steps have been taken by some airports, the deficiency is that the solutions are all local. A federated credential system would significantly enhance airport security, be more convenient for airport employees and reduce the cost of having to issue multiple credentials.

Some airline crews carry a Known Crew Member credential that contains a barcode, but they also must present an employee ID card and a third credential such as a driver's license or passport to a TSA agent. Unfortunately for airport security, barcode technology is more appropriate for low-risk environments. This creates a significant security gap in that the TSA cannot be sure that the employee presenting the KCM card has not compromised the system. It is possible that someone could create a fraudulent KCM card, employee card and driver's license.

As the ASAC and TSA have recognized, the best security relies on a risk-based approach and one that is layered so that a breach in any one layer does not compromise security. The use of CCTV cameras, physical access control systems and physical barriers are just some of the layers in use at airports today.

The ASAC report also recommends a Work Schedule Audit to reconcile the badge holder's work schedule with the access control systems during a specified period to identify access anomalies or irregularities such as an employee using his or her badge at the airport outside of their normal work hours. Unfortunately, this looks into the past and will not detect such anomalies in real-time when a security breach might be occurring.

The security industry has developed identity management systems that serve as systems of record for every airport worker and will detect anomalies or deviations from normal work patterns in real time. These systems will alert airport security as anomalies/deviations occur so they can be investigated immediately if necessary.

Equally important, such identity management systems, which are being used by several major airports throughout the country, are structured so that they enforce all TSA guidelines for badging and meet Airport Security Policy as determined by each airport. And, these same systems can automatically ping FBI and other criminal databases to ascertain, in real-time, if an airport worker has been arrested, eliminating the need for 100 percent background checks of all employees on a recurrent basis.

These same systems can conduct audits recommended by the ASAC to ensure that an Authorized Signatory is in compliance with badging requirements for employees. And, in the future, as TSA explores the use of social media to track and assess emerging threats that may pose a risk to aviation, identity management systems could prove to be a valuable tool in automating this vital undertaking.

It's important to remember that the credential is just one piece of the security solution. The infrastructure must be in place, including an identity management system, to authenticate and authorize badge holders in an always-connected environment.

I want to thank the Committee again for including the security industry in this important discussion. We welcome the opportunity to contribute to improving aviation and airport security nationwide.

I look forward to your questions.

Kathleen M. Carroll

Kathleen Carroll is Vice President, Government Affairs for HID Global, a worldwide leader in secure identity solutions. Carroll serves as an ambassador, spokesperson and representative for HID Global. She oversees the company's privacy and policy initiatives to support its brands around the world. She also works to support public policies that address physical security, cybersecurity and privacy at the national and international levels.

As part of her responsibilities, Carroll chairs the Security Industry Association's (SIA) Government Relations Committee which works to educate legislators, business leaders and consumers about security technologies and their benefits across a spectrum of applications, including identity management, physical and logical (cyber-security) access control, food and drug safety, child safety, and patient safety. Carroll also sits on the National Security Task Force at the U.S. Chamber of Commerce.

An Advisory Board member for the Identity Center at the University of Texas at Austin she is a frequent speaker at industry events, discussing the intersection of privacy and technology and the implications for both the public and private sector as this issue rapidly evolves. In addition, she chairs the Privacy and Public Policy working group within the International Biometrics and Identification Association (IBIA). Carroll also serves on the Advisory Board for Mission 500, a non-profit organization dedicated to serving the needs of children and communities in crisis.

A magna cum laude graduate of Temple University, Carroll earned a BA in Journalism. She is a member of the International Association of Privacy Professionals and a Certified Information Privacy Professional and a Certified Information Privacy Professional/Government.