STATEMENT OF
CAPTAIN SEAN CASSIDY
FIRST VICE PRESIDENT
AIR LINE PILOTS ASSOCIATION, INTERNATIONAL
BEFORE THE
SUBCOMMITTEE ON TRANSPORTATION SECURITY
COMMITTEE ON HOMELAND SECURITY
UNITED STATES HOUSE OF REPRESENTATIVES
WASHINGTON, DC
MAY 16, 2012

Access Control Point Breaches at Our Nation's Airports: Anomalies or Systemic Failures?

Air Line Pilots Association, International
1625 Massachusetts Avenue, NW
Washington, DC 20036
(202) 797-4033

STATEMENT OF
CAPTAIN SEAN CASSIDY
FIRST VICE PRESIDENT
AIR LINE PILOTS ASSOCIATION, INTERNATIONAL
BEFORE THE
SUBCOMMITTEE ON TRANSPORTATION SECURITY
COMMITTEE ON HOMELAND SECURITY
UNITED STATES HOUSE OF REPRESENTATIVES
ON
"ACCESS CONTROL POINT BREACHES AT OUR NATION'S AIRPORTS: ANOMALIES OR SYSTEMIC FAILURES?"
May 16, 2012

Mr. Chairman and Ranking Member Jackson-Lee, thank you for the opportunity to testify. The Air Line Pilots Association, International (ALPA), representing more than 53, 000 pilots flying for 37 airlines in the United States and Canada, is the world's largest professional pilot association and the world's largest non-governmental aviation safety organization. We are the representative for the majority of professional airline pilots in the United States with a history of safety and security advocacy spanning more than 80 years. As the sole US member of the International Federation of Airline Pilots Associations (IFALPA), ALPA has the unique ability to provide active airline pilot expertise to aviation safety and security issues worldwide, and to incorporate an international dimension to safety and security advocacy.

OVERVIEW

We applaud the Subcommittee's demonstrated interest in airline and airport security by holding this hearing on airport access and other, related subjects.

Maintaining and enforcing effective control of access to sterile and secure airport areas is critically important to the safety and security of the airline industry and the traveling public. The Transportation Security Administration (TSA) reviews and approves mandated Airport Security Programs (ASPs) which must be followed by our nation's certificated, commercial airports.

ASPs must delineate effective measures designed to preclude unauthorized access to sterile and secure areas, and also must provide effective response protocols in those instances where unauthorized access is attempted or occurs.

To comply with these mandated security measures, airports utilize a variety of mechanisms, to include: Security Identification Display Area (SIDA) protocols; security training and challenge protocols for SIDA badge-holders; perimeter fencing and physical barriers; sophisticated technologies to prevent and detect unauthorized entry into sterile and secure areas; law enforcement patrol and response; and, interior access control systems which incorporate both technological and human resources.

Airport screening checkpoints play a prominent role in an airport's security plan, providing access and screening controls to airport sterile areas for passengers, aviation and airport workers. Airports work in close partnership with the TSA to facilitate the checkpoint screening process.

Accompanying these required airport access control measures dictated in the ASP are certain other TSA policy mandates, normally implemented through Security Directives (SDs) or Emergency Amendments (EAs), which obligate airports and aviation workers to enforce and follow prescribed protocols related to accessing sterile and secure airport areas, and, at times, dictating specific protocols aviation workers must follow as pertains to traditional checkpoint screening, or, alternative forms of approved screening prior to entering sterile and secure airport areas.

The ALPA- and Airlines for America-sponsored security screening system for pilots, Known Crewmember (KCM), is an example of a government-approved, alternative means of access to sterile areas of airports which is available to pilots who comply with KCM requirements. KCM has been implemented at 7 airports thus far, with 11 more that have been identified to receive the system soon and many more thereafter. ALPA and A4A have encouraged the TSA to include flight attendants in this program, as they should be part of risk-based security.

It has been ALPA's general experience that TSA and airport authorities do a very good job in controlling and preventing unauthorized access to sterile and secure airport areas. There have been some documented failures in this regard, causing inconvenience to passengers and resulting in a negative impact on the timeliness of airline and airport operations. However, we know of no such instances which involved persons who possessed the intent to do harm to the aviation industry. Based on the specifics of these reported incidents, we believe that both TSA and airports have developed sound strategies intended to prevent their reoccurrence.

It has also been ALPA's experience that, in general, aviation workers comply with government requirements regarding entry into airport sterile and secure areas. Because of practical constraints or operational needs, those regulations do not require all such workers to undergo traditional checkpoint screening protocols prior to entry, but apply alternative means of screening instead. It is normally in this context that discussion ensues regarding the "insider threat" to aviation.

Source of the Threat

The insider threat to passenger and all-cargo aviation operations has always existed in aviation security; it is not a new threat. It is one that must always be addressed, so that the risk of this threat causing a serious event is minimized to the maximum, practical extent. Notwithstanding the advances that have been made in passenger and cargo screening since 9/11, and the reliability of most aviation employees, a concentrated effort is needed to identify and eliminate threats posed by individuals who have access to commercial aircraft and their payloads.

Shortly after the Christmas Day 2009 underwear bomber's thwarted attack on NWA Flight #253 as it approached Detroit, ALPA published a white paper entitled *Meeting Today's Aviation Security Needs: A Call to Action for a Trust-Based Security System.* In it, we cited the need for a more comprehensive, threat-based approach to aviation security, stating: "The insider threat to the aviation industry must not be overlooked or minimized. It must be addressed along with enhanced screening capabilities; background checks should be conducted on all those with access to our airplanes."

Historically, the insider threat has been well-documented, both internationally and domestically. Al Qaeda in the Arabian Peninsula (AQAP) has attempted to facilitate the hiring of flight attendants, baggage handlers, and airport security personnel, and in 2010, a Taliban sympathizer gained employment as a baggage handler at a U.S. carrier and traveled to Afghanistan to provide assistance in fighting against U.S. forces.

While we believe that the vast majority of individuals employed by the airlines and government agencies at the airport are upright, responsible and trustworthy, no organization is immune from the possibility of employing individuals who engage in criminal behavior. Criminal organizations in the United States have regularly used airport, airline, government and contract employees to facilitate criminal activities in the airport environment, which include, but are not limited to, drug trafficking, contraband smuggling, theft and prostitution. In March, a security officer in Buffalo, NY was criminally charged with allowing passengers to pass through screening checkpoints while using false identification, and as recently as last month, federal drug agents arrested two former and two current security personnel at Los Angeles International Airport on drug trafficking and bribery charges.

Fortunately for the traveling public, the insider threat has primarily been associated with the perpetration of criminal rather than terrorist activity. However, just as a criminal organization can infiltrate a segment of the aviation work force or circumvent existing security procedures, so too can a terrorist organization. Whether breached by a willing participant who is working for a criminal or terrorist organization, or an unwitting dupe believing he is simply facilitating a criminal rather than a terrorist act, existing weaknesses which facilitate these dynamics must be identified and corrected.

Vulnerability and risk associated with the insider threat is magnified because risk-based security measures have not yet been applied to the extent that they are needed. One example: the May 2006 Air Cargo Final Rule did not require *all* airports which serve all-cargo airline operations to establish Security Identification Display Areas (or SIDAs). Many persons with access to air operations areas of these airports and to wide-body cargo aircraft are background-vetted only by means of a biographic-based Security Threat Assessment (STA) process, rather than by means of a fingerprint-based Criminal History Records Check (CHRC) which is required for similar employee categories in the passenger airline domain.

This lack of standardized application of fingerprint-based CHRCs in background-vetting of aviation workers exists even though the government has publicly acknowledged that a fingerprint-based CHRC provides a greater degree of security than an STA, and that there should be congruency in background vetting for workers in functions that present similar security concerns, such as checked baggage screeners and cargo screeners. As a result of this imbalance in background-vetting standards, many persons holding positions of trust in the all-cargo domain, and who have unescorted access to cargo aircraft, the goods they carry and to air operations areas of airports, are not vetted to the same standard as persons occupying equivalent positions in the passenger aviation domain.

There is long-established precedent for using fingerprint-based CHRCs in determining an individual's suitability for hiring in a security-sensitive position. Numerous employment categories exclude convicted felons from eligibility, deeming them to be unsuitable candidates due to security concerns, character issues, and recidivism rates. The difference between undergoing CHRC-based background vetting as opposed to a STA is significant when viewed in terms of the dangers presented by the insider threat. Without use of a fingerprint-based CHRC, no reliable determination can be made as to whether a person has been convicted of any of the 28 prohibited crimes that are described in 49 CFR §1544.229, and which preclude unescorted access to secure airport areas. This lack of standardization between the background-vetting processes applied to workers employed by passenger airlines and all-cargo carriers unnecessarily creates yet another challenge in mitigating the insider threat to aviation.

Reasonable Expectations

To effectively mitigate the problem of the insider threat to aviation, we must begin with reasonable expectations, have a good understanding of the industry's operational environment, acknowledge that there can never be total elimination of risk and accept the fact that the best we can hope to achieve is reasonable mitigation of the threats we face. It is also necessary to recognize that a certain degree of trust must always exist within the framework of securing the aviation domain. For the system to work, we have to trust Federal Security Directors, Transportation Security Officers, airport law enforcement officers, air traffic controllers, pilots, flight attendants, aircraft mechanics, et al. If we did not, the industry would be paralyzed.

History has demonstrated that "trust" is a very fluid dynamic which offers no guarantees. Aldrich Ames and Robert Hanssen attained the highest levels of trust within their respective agencies, but ultimately compromised the values they had sworn to protect and the security of their nation. Fortunately, such events are extremely rare and despite the uncertainties which will always accompany the allocation of "trust," so doing is a necessary component of any security system. It is in this context that the concept of "trust, but verify" takes on significance.

Recommendations for Mitigation

Since its creation following the 9/11 attacks, the TSA has continued to evolve its passenger screening measures in an attempt to address the challenges posed by an intelligent, adaptive terrorist adversary. We have witnessed the evolution of Advanced Imaging Technology and the increased use of Behavioral Detection Officers. Regardless of the tremendous advances in airport screening capabilities, however, we only have to recall the incident of the infamous "underwear bomber," or last week's reports that intelligence and law enforcement agencies had identified and interdicted an IED created entirely of non-metallic material reportedly designed by an AQAP master bomb-maker to be detonated by a suicide bomber aboard an aircraft.

Although technology plays an integral role in the aviation security process, it is not a stand-alone solution. TSA Administrator John Pistole has recognized this fact by applying a more risk-based, threat-driven approach to aviation security, as evidenced by his support of the Known Crewmember program and other special screening programs such as Global Entry, Pre-Check, I-Step, SPOT and behavioral detection techniques. The DHS public message of "If you see something, say something..." is a valuable public awareness campaign to help mitigate the threat of terrorism.

Harnessing Existing Resources

Aviation workers, which number in the hundreds of thousands, represent a vast and under-utilized resource in protecting the aviation domain, to include combating the insider threat. Commercial pilots, all of whom have undergone security awareness training as part of their employment, know their segment of the aviation industry and can sense anomalies whether commuting for work, on personal travel or flying their assigned routes. Just as a police officer knows the beat he patrols and the mailman knows the neighborhood in which he delivers, so does the pilot know his or her normal work environment. As such, pilots should be considered assets in identifying threats to the industry, including insider threats, and treated as part of the solution rather than being viewed as part of the problem. This logic can be applied to other classes of aviation workers who frequent the airport domain: flight attendants, mechanics, caterers, fuelers, baggage handlers, airport service providers, et al.

In the late 1990's, ALPA served on the government/industry Employee Utilization Working Group (EUWG) for the purpose of identifying guidelines to be followed by aviation sector

employees to enhance security. One of the recommendations ALPA made to that group was to focus on the largely untapped resource of airport, airline and other tenant employees. All of the individuals who work at an airport, regardless of position, background and experience, and can usefully serve as the 'eyes and ears' of security.

Regrettably, the EUWG's recommendations have been largely ignored, but we believe that this hearing provides an opportune time to revisit them, because they are still valid:

- Encourage and assist airports and air carriers to develop and implement security awareness programs which emphasize the "team" concept
- Encourage each airport and airline to employ or designate an existing employee as a security training manager
- Create a standing security awareness working group comprised of government and industry representatives for the specific purpose of enhancing employee's security awareness and compliance
- Perform human factors research into why security lapses occur, applying lessons learned from that research to future employee awareness training efforts
- Encourage certain employee groups (e.g., baggage handlers) to have their members serve as candidates to be used as a security observer/auditor for a few hours each month on a rotating basis when schedules allow. Employees should be utilized in this fashion in order to make them more security conscious
- Create a common, easily remembered, and dedicated phone number for specific employee use at airports for reporting of suspicious behavior or security breaches
- Maintain a repository of employee utilization and security awareness media, including videos

Just as practical experience has shown that the vast majority of airline passengers have no evil intent and represent no threat to aviation, the same can be said for the vast majority of aviation workers. By properly vetting, training, harnessing and empowering them, much can be done to counter the insider threat.

The accomplishment of this goal will require a paradigm shift within the aviation domain. Just as the airline industry has placed great emphasis on the use of Safety Management Systems (SMS) in order to achieve and maintain aviation's excellent safety record, similar emphasis must be placed on the development and maintenance of a comprehensive security management system.

The successful completion of this task will require true buy-in from the leadership of critical aviation stakeholders such as airlines, airports and regulators, and their definitive action in the establishment and enforcement of a true security culture within their respective organizations. It will require these entities to invest more resources in and place more emphasis on providing meaningful, practical security training to employees and their empowerment as valued security resources, rather than simply "checking the box" in meeting government mandates regarding

the length and content of security training. Only in this way can a true security culture be established.

CONCLUSIONS

One hundred percent physical screening of individuals entering secure/sterile areas of airports is not the answer to the insider threat. A highly-developed, systematic and reliable method of employee vetting, including fingerprint-based criminal history background checks (CHRC) of every employee with unescorted access to passenger and cargo aircraft, air operations areas, baggage and cargo should be implemented to support a risk-based approach to identify "evil intent." To this end, full SIDA requirements must be mandated for all airports serving FAR part 121 all-cargo operations. In addition, fingerprint-based CHRCs must accompany the STA process in the background vetting of all individuals who have unescorted access to all-cargo air operations areas, aircraft and the cargo they carry.

If the leadership of critical aviation stakeholder organizations and regulators commit themselves to following through on the aforementioned recommendations, and if aviation workers are properly vetted, provided the appropriate training and reporting mechanisms and then empowered, they can be counted upon to counter the insider threat.

This approach to aviation security, coupled with other more traditional methodologies such as the use of random inspections, employment of technological assets, such as surveillance and detection equipment, will do much to mitigate the insider threat, at very reasonable cost.

ALPA is grateful for the opportunity to be heard on this important matter and to provide its views to the Subcommittee.

# # #