STATEMENT OF

CAPTAIN TIM CANOLL

PRESIDENT

AIR LINE PILOTS ASSOCIATION, INTERNATIONAL

BEFORE THE

SUBCOMMITTEE ON TRANSPORTATION AND

PROTECTIVE SECURITY

OF THE

COMMITTEE ON HOMELAND SECURITY

U.S. HOUSE OF REPRESENTATIVES

SEPTEMBER 27, 2018

"INSIDER THREATS TO AVIATION SECURITY: AIRLINE AND AIRPORT PERSPECTIVES"

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

STATEMENT OF
CAPTAIN TIM CANOLL
PRESIDENT
AIR LINE PILOTS ASSOCIATION, INTERNATIONAL
BEFORE THE
SUBCOMMTTEE ON TRANSPORTATION AND
PROTECTIVE SECURITY
OF THE
COMMITTEE ON HOMELAND SECURITY
U.S. HOUSE OF REPRESENTATIVES
SEPTEMBER 27, 2018
"INSIDER THREATS TO AVIATION SECURITY:
AIRLINE AND AIRPORT PERSPECTIVES"

The Air Line Pilots Association, International (ALPA), represents more than 60,000 professional airline pilots who fly for 34 airlines in the United States and Canada. ALPA is the world's largest pilot union and the world's largest non-governmental aviation safety and security organization. We are the recognized voice of the airline piloting profession in North America, with a history of safety and security advocacy spanning more than 85 years. As the sole U.S. member of the International Federation of Airline Pilots Associations (IFALPA), ALPA has the unique ability to provide active airline pilot expertise to aviation security issues worldwide, and to incorporate an international dimension to security advocacy. ALPA has a long and distinguished record of accomplishments in aviation security which include being a forceful advocate for means to end the hijacking epidemic in the 1960's-70's, led the development of the Federal Flight Deck Officer program and the Known Crewmember program following the attacks of 9/11, and we have been vocal and active on the issue of the insider threat—the subject of today's hearing—for many years.

Background

ALPA sincerely appreciates Chairman Katko's leadership in the aviation security arena and applauds the subcommittee's interests in reducing the threat posed by anyone who may have nefarious intentions which could be exploited while working inside the aviation system. According to the Department of Homeland Security's (DHS's) September 14, 2018, *National Terrorism Advisory System Bulletin*, "We continue to face one of the most challenging threat environments since 9/11, as foreign terrorist organizations exploit the Internet to inspire, enable, or direct individuals already here in

the homeland to commit terrorist acts." Terrorism analysts inform us that according to current intelligence, aviation continues to be the "gold standard" target of terrorist groups, so the timing and subject of this hearing are very appropriate.

For purposes of this statement, we identify an "insider" as someone with authorization and unescorted access to secured areas of an airport and/or aircraft. Certainly, there is potential for insiders employed in positions of trust within the commercial aviation arena to harm passengers, crews, aircraft and cargo. Fortunately, the number of insider threat incidents is exceptionally low in the U.S., but the government and industry must continually be on their guard against this threat vector and work tirelessly to stay ahead of it.

Aviation security, like many other types of security, is built on a foundation of trust in the individual. Individuals employed in security-sensitive industries, like aviation, must pass extensive background and prior employment checks plus criminal history records checks. Those who pass those checks are issued identification media, access codes and other means to open locked doors, and the scope of their unescorted access is defined according to their job function. Generally, this system works well for the vast majority of trusted employees, but it certainly is not perfect as has been demonstrated on a number of occasions, most recently with an apparent theft and suicide of an airline employee using a company aircraft in Seattle.

The Nature of the Insider Threat

Fortunately, there are very few incidents of insider attacks against aviation which is a testament to the security systems in place in the U.S. and most nations around the world. The types of threats that exist can be:

- malicious—the insider seeks to aid or conduct an act which is intended to cause death, injuries and/or harm to property
- complacent—the insider takes a lax approach to policies, procedures, and potential security risks
- unwitting—the insider is not aware of security policies, procedures and protocols which expose the organizations/agency to external risks
- from anyone who has authorized access to the Security Identification Display Area (SIDA) or Air Operations Area (AOA), which includes:
    - Aircrew
    - Technicians
    - Ground handlers (baggage/cargo handlers, gate agents, aircraft servicers, etc.)

- Vendors (restaurants, construction, transportation, etc.)
- Law enforcement and security personnel

In 2014, it was reported that several aviation employees involved in an alleged gun-smuggling ring had been arrested for using commercial airliners to transport prohibited items between two East Coast airports. Even though there was no discernible terrorist threat against commercial aviation, this criminal enterprise created significant concern for the public, government and industry. Two other examples of insider threats are as follows:

- In 2013, the FBI successfully established a sting operation in which agents, posing as terrorist co-conspirators, assisted a general aviation avionics technician in bringing what he believed was a bomb onto the tarmac to destroy aircraft. The perpetrator was arrested and ultimately sentenced to 20 years in prison.
- In February 2016, a bomb detonated on Daallo Airlines Flight 159 twenty minutes after departing Mogadishu, killing the passenger who had brought it onboard. In May of that year, two men were found guilty in court of planning the plot, one of whom was a former security official at the airport, and eight other airport workers were convicted of aiding the plot.
- In May 2017, an American citizen and U.S. Air Force veteran who had worked as an aircraft mechanic for a U.S. legacy airline and other carriers, was indicted on charges of supporting ISIS and sentenced to 35 years in prison.

In addition to improvised explosive devices, threats from insiders could also come via the use of other prohibited items including firearms, knives and other types of weapons, plus hijackings. Virtually undetectable threats, however, could come in the form of aircraft sabotage by those with knowledge of aircraft vulnerabilities, or cyber-attacks launched distantly. Although airline pilots are focused mostly on the security of ground and inflight aircraft operations, vulnerabilities to active shooters and other types of threats from insiders exist within airport terminals and the AOA. As in the case of the 2014 gun-smuggling ring, insiders may also plot and/or carry out criminal activity (e.g., theft) that is not aimed against aviation interests, but is still of concern due to the potential for terrorists to compromise security through the assistance of such actors.

Insider threat vulnerabilities exist in airport terminals, which may be relatively soft targets with large crowds at passenger pick-up and drop-off areas. Other areas which present particular vulnerabilities with congregations of passengers include ticketing/check-in counters, security screening queues, baggage claim areas, and gate areas.

Aircraft are vulnerable to sabotage while on the ground and while in flight. During periods of inactivity, or during off-peak hours at an airport, not all aircraft are parked within SIDAs where multiple security layers are most prevalent. Also, one of the most vulnerable moments during flight happens when the cockpit door is opened, and flight crew exit or enter for required rest breaks or physiological needs. ALPA has vigorously advocated for several years for a requirement for installed secondary barriers on passenger aircraft: lightweight devices, which protect the flight deck from attack during the time that the cockpit door is opened for operational reasons during flight. Airlines are presently permitted to develop their own procedures using service carts and flight attendants to block access to the cockpit when the door is opened, but DHS-conducted testing in the mid-2000's demonstrated the inadequacy of those measures.

Insider threats may also include cybersecurity attacks. We have seen both the operational and financial consequences of the loss of an airline reservation system, or the interruption to ATC services which are computerized. Aircraft are highly computerized machines with the bulk of their systems reliant on electronic primary and back-up sub-systems. With numerous personnel accessing the aircraft while it is on the ground and in the air via Wi-Fi, satellite, or a connected device, the introduction of a malicious virus is a possibility which government and industry are taking very seriously.

<u>Insider Threats to All-Cargo Operations</u>

We would like to highlight the security vulnerabilities that exist for all-cargo operations which are distinct from those of passenger operations. All-cargo operations have different regulatory requirements in a number of areas including the following, which make them more susceptible to insider threats:

- The TSA has developed and mandated the teaching of a security training guidance document known as the "Common Strategy" for passenger airlines and crews. The TSA has also established, but not mandated, the teaching of equivalent security training guidance known as the "All-Cargo Common Strategy" for all-cargo airline employees and crews. Government-approved security training, equivalent to that required in the passenger domain, should be required for flight crews and ground personnel supporting all-cargo flight operations.
- In 2003, Congress passed the Vision 100—Century of Aviation Reauthorization Act (P.L. 108-176), which included a provision requiring a "training program for flight and cabin crew members to prepare the crew members for potential threat

conditions." These provisions were not and have not been required for all-cargo crews; they are needed to help guard against insider and other threats.

- Also, in 2003, Congress passed an appropriations bill (P.L. 108-7), which included a provision stating that, "No funds appropriated in this Act may be used to apply or enforce a regulatory requirement for strengthening of flight deck doors" on other than passenger aircraft. That year, the FAA issued a rule requiring flight deck security for all-cargo operations via an installed, reinforced flight deck door or enhanced security measures to screen personnel with access to the aircraft and cargo. It is ALPA's view that flight deck doors are needed on all-cargo aircraft—just as they are on passenger aircraft—as an additional layer of security, and the AMOC needs to be rescinded. Hardened flight deck doors are needed on every airplane, cargo and passenger. That is our best directed deterrent in preventing another 9/11.
- The TSA has developed and mandated the teaching of a security training guidance document known as the "Common Strategy" for passenger airlines and crews. The TSA has also established, but not required, the teaching of equivalent security training guidance known as the "All-Cargo Common Strategy" for all-cargo airline employees and crews. Government-approved security training, equivalent to that required in the passenger domain, should be mandated for and tailored to the needs of flight crews and ground personnel supporting all-cargo flight operations.
- Unlike passenger aircraft which are mandated to be equipped with hardened flight deck doors, all-cargo aircraft are not required to have them unless they had a flight deck door on or after January 15, 2002. However, new, widebody aircraft are being operated by U.S. all-cargo operators that do not have a flight deck door at all.
- The full all-cargo aircraft operators' standard security plan is written on the basis of an installed, hardened, cockpit door. The plan needs to be updated/amended to reflect the reality of the cargo equipage requirements and reality, and training needs to be required for all affected employees on the plan.
- In 2006, the Transportation Security Administration (TSA) issued new regulations concerning all-cargo operators which created a requirement for those operating aircraft of 100,000 pounds or greater to conduct loading and unloading operations within a SIDA. However, loopholes in the regulations allow part-time SIDAs, and smaller all-cargo aircraft which "feed" cargo to large aircraft to be operated outside of a SIDA at certain airports.
- All-cargo operators have been issued deviations to the Federal Aviation Regulations allowing greater access by non-pilots to aircraft and flight decks. Yet in 2002, the FAA itself referred to the flight deck as "the nerve center" of the

operation. The agency further stated that any access request "shall be strictly and narrowly interpreted."

- Some allowed access—which includes foreign nationals with access to the cockpits of some all-cargo transport category aircraft during flight—are vetted on the basis of a Security Threat Assessment (STA), not a fingerprint-based criminal history records check, as is required for insiders within the SIDA.
- The Federal Flight Deck Officer (FFDO) tactics, techniques and procedures trained by TSA do not reflect the realities of an attack coming onboard an aircraft without a hardened door, and they need to be amended for that purpose. This information has been conveyed to responsible parties in TSA.

Actions to Address the Insider Threat

Commercial aviation has greatly increased its safety record using predictive data which helps identify potential or actual risk. Similarly, TSA and the aviation industry, including ALPA, have been working for several years on the development of more advanced means of predicting if and when a person will become an actual threat to security. The U.S. has made significant strides toward obtaining a better understanding of the trustworthiness of individuals working in airport sensitive areas, and elsewhere of course, since the 9/11 attacks. This has been accomplished, in part, by the development and use of the FBI's Rap Back service which, as described by the Bureau, "allows authorized agencies to receive notification of activity on individuals who hold positions of trust…thus eliminating the need for repeated background checks on a person from the same applicant agency. Prior to the deployment of Rap Back, the national criminal history background check system provided a one-time snapshot view of an individual's criminal history status. With Rap Back, authorized agencies can receive on-going status notifications of any criminal history reported to the FBI after the initial processing and retention of criminal or civil transactions." TSA also performs recurrent checks against the Terrorist Screening Center's watchlist and other databases to identify any person who is known or suspected of being involved in terrorist activities.

Perhaps most importantly, TSA has adopted a risk-based approach with the goal of consistently applying it to all aspects of the agency's mission. This replaces the one-size-fits-all security, which was in place on 9/11, and includes consideration of the individual and his or her role within aviation in the development of security requirements and policies. ALPA has been advocating for a risk-based security paradigm for about two decades and has been pleased to work with this Committee to improve our nation's aviation security infrastructure and protocols.

In 2009, TSA initiated an Insider Threat Task Force, and in 2013 created a new Insider Threat Program, which includes an Insider Threat Unit that follows up on threat incidents, inquiries and tips. Two years later, the agency chartered the Insider Threat Advisory Group (ITAG) of TSA subject matter experts. Earlier this year, TSA asked the Aviation Security Advisory Committee to create a new Insider Threat Subcommittee, on which ALPA participates. The subcommittee has met twice in the past few months and is presently anticipating a request from TSA leadership to expound on and make recommendations concerning the threat posed by insiders with access to aircraft, as was demonstrated in the Horizon aircraft-theft tragedy, along with any new or revised recommendations.

Relatedly, TSA requested ASAC in 2014 to create an Employee Access Working Group, on which ALPA was represented, that delved into the physical screening of employees at entrances to secured areas and other means of minimizing the risk of insiders. The WG reported its findings to the TSA's leadership the following year along with 28 separate recommendations for improving countermeasures against the potential threats posed by insiders. Those recommendations covered a wide range of different aspects of improvements to thwart the threat and many of them have been implemented or are in the process of being implemented.

Horizon Air Tragedy

A matter of great interest continues to be the circumstances of the Horizon Air tragedy near Seattle-Tacoma International Airport, in which a company ramp employee, named Richard Russell, commandeered a Q400 aircraft and after a period of flight, crashed the airplane into the ground. Unanswered questions remain about why this individual committed such an outrageous act, and how he was able to do so. What we know is that the employee is reported to have passed all company and airport vetting checks to obtain employment and required access badges. We also know that he gained access to the aircraft that he eventually stole in an area of the airport in which he was authorized to work unescorted.

Melbourne, FL Security Breach

While not specific to an insider threat, under current deviances for cargo operators, nothing would prevent a security breach like the one in Melbourne, Florida a few days ago from having an impact on cargo security. If there are non-trusted insiders with access because of weak SIDA rules, background checks, and vetting for all cargo operators creates opportunity. This event demonstrates methodology and means,

and **intent**. Additionally, it highlights the ability for people to gain access to SIDAs and it is only a matter of time before they realize that cargo wide body aircraft have no cockpit doors. Media reports indicate that the individual wanted to do harm with the aircraft. Attempted commandeering seems to be a "trending" risk, which under current rules makes cargo specifically vulnerable.

While we are collectively waiting for the answers which will likely come at some future date, one area of improvement that ALPA believes is worth pursuing is making mental health resources available to all aviation insiders. Since the beginning of this year, ALPA has expended considerable resources on the development of a new, peer-reviewed support program. It is our belief that this program, and others like it, will help save lives of aviation employees and others.

Conclusions

The insider threat is one that has existed as long as there have been aviation industry employees and one that will be always be a component of the industry. The threat today is manageable, however, because of efforts being made by TSA and the industry to collectively stay abreast of it. However, improvements are needed, particularly within the all-cargo arena which does not have the same level of security as passenger operations. We urge this Subcommittee to continue to exercise its oversight and leadership and help ensure that all sectors of commercial aviation are adequately protected from external and internal threats.

# # #