

**Air Line Pilots Association,
International**

WHITE PAPER:
**Recommendations
For Improving the
Security of
All-Cargo Air
Operations**

August 2011

ALPA WHITE PAPER

AIR LINE PILOTS ASSOCIATION, INTERNATIONAL

1625 Massachusetts Avenue, N.W., Washington, D.C. 20036
703-481-4440 ■ media@alpa.org ■ www.alpa.org

Recommendations for Improving the Security of All-Cargo Air Operations

An effective air-cargo protective system must focus on the components of the entire supply chain, anticipate opportunities for, and provide reasonable measures to prevent or interrupt, the perpetration of malicious acts.

The Air Line Pilots Association, International (ALPA), is the world's largest airline pilot union, representing more than 53,000 pilots who fly passengers and cargo for 39 airlines in the United States and Canada. ALPA has long supported the concept of "One Level of Safety and Security" in regulations, policies, and procedures related to all aspects of airline operations, including carrying cargo on both passenger and all-cargo airliners. This document provides historical perspective on recent efforts to secure the air-cargo supply chain and then offers recommendations for improving security. To learn more about ALPA, visit the Association's website, www.alpa.org.

Overview

The air-cargo supply chain is a complex, multifaceted mechanism. It begins when a shipper tenders goods for transport, and it potentially involves numerous intermediary organizations such as Indirect Air Carriers (IACs), freight forwarders, and other industry personnel who accommodate the movement of goods. Ultimately, a shipment is received by air carrier personnel, loaded on an airliner, and delivered to its intended destination.

An effective air-cargo protective system must focus on the components of the entire supply chain, anticipate opportunities for, and provide reasonable measures to prevent or interrupt, the perpetration of malicious acts. Such a system must certify the integrity of the goods that are offered and the reliability of the shipper, verify the trustworthiness and proper training of all personnel who maintain access to shipments, and ensure a reliable, secure operating environment as tendered goods move through the system.

Unfortunately, the aviation industry has yet to develop and implement an all-encompassing cargo security system that provides equal protections in the carriage of cargo on passenger and all-cargo aircraft. Since the events of September 11, 2011, government efforts have primarily been focused on improving the protection of passenger airline operations, including the transport of cargo, while relegating all-cargo airline operations to a secondary status. Tremendous progress has been made in better securing the portion of the air-cargo supply chain that is facilitated by passenger airline operations. Because of remaining, demonstrable vulnerabilities impacting all-cargo air operations and the lack of parity in regulatory requirements that affect them, the Air Line Pilots Association, International, believes it is time to take affirmative and critically needed corrective action.

Background

Immediately following the 9/11 terrorist attacks, the U.S. Congress acted to further protect the nation's infrastructure by establishing the Department of Homeland Security (DHS) and the Transportation Security Administration (TSA) and by enacting numerous regulations affecting aviation security. Transport Canada (TC) likewise created the Canadian Air Transport Security Authority (CATSA). Subsequently, various government-sponsored working groups that were composed

Air Cargo Security



... the Final Rule failed to apply an equal standard as is mandated for the security of passenger airline operations, resulting in a clear lack of regulatory parity.

of aviation and other security experts were convened in both countries for the purpose of bolstering protective measures that are primarily directed at the security of *passenger* airline operations. Some of the more notable improvements that resulted included: enhanced airport checkpoint screening; dramatic expansion of the Federal Air Marshal Service (FAMS) and the creation of the Canadian Air Carrier Protective Program (CACPP); requirements for hardened flight deck doors; revised security training guidance for passenger flight crews; and the creation of the Federal Flight Deck Officer (FFDO) program.

In the years that have passed since 9/11, some notable improvements in the security of the all-cargo air domain have also been realized. In Canada, the previously used “Known Shipper” system was replaced by a greatly expanded program based on the concept of the “Regulated Agent,” which involved vetting of both shippers and freight forwarders and assigned specific responsibilities for cargo screening, including the concept of the “accountable executive” designated to be personally responsible for the cargo security program. In the United States, based on years of work by the Aviation Security Advisory Committee (ASAC) and its Air Cargo Working Groups, the TSA published the Air Cargo Security Requirements: Final Rule in May 2006. It declared the “hostile takeover of an all-cargo aircraft leading to its use as a weapon” to be a critical risk. Through it, a number of significant improvements to the security of the air-cargo supply chain were mandated, requiring airports, domestic and foreign airlines, and indirect air carriers to implement meaningful additional security measures.

For the first time, per the rule’s regulations, all-cargo airlines operating aircraft with a certificated takeoff weight of more than 45,500 kg (100,310.3 lbs) were required to comply with the standardized security requirements of the Full All-Cargo Aircraft Operator Standard Security Program. This mandate was historic, as all-cargo operators had previously been permitted to develop their own security programs on an individual basis and to apply for government approval.

The Final Rule also expanded Security Identification Display Area (SIDA) requirements at some—but not all—airports supporting cargo airline operations. It specified that any airport operating under a full security program required by CFR Section 1542.103(a) must extend SIDA protections to “each part of the air operations area that is regularly used to load cargo on or unload cargo from an aircraft that is operated under a full program or a full all-cargo program.”

Although the Final Rule produced major improvements in the security of the air-cargo supply chain and cargo airline operations, it failed to apply an equal standard as is mandated for the security of passenger airline operations, resulting in a clear lack of regulatory parity. In January 2005, ALPA voiced its concerns with respect to this issue in its response to a Notice of Proposed Rulemaking (NPRM), published in the *Federal Register* on Nov. 10, 2004, entitled Air Cargo Security Requirements (Docket No. TSA-2004-19515).

In summary, a number of stakeholders in the all-cargo airline industry and the supply chain that feeds it have been exempted from compliance with many of the stricter security policies that are mandated for

SIDA requirements detail perimeter security protocols, clearly define entry and exit procedures, dictate specific identification display and ramp security procedures, and are predicated on a mandatory 10-year, fingerprint-based criminal-history record check (CHRC) for all employees who maintain unescorted-access privileges within the SIDA.

the handling of cargo in passenger airline operations. What follows is a description of the most urgently needed security enhancements for the all-cargo industry, which are provided with the understanding that improvements must accommodate the flow of commerce and be threat-driven, affordable, and cost-justified.

Recommendations

Security Identification Display Area (SIDA) for All-Cargo Operations

The Air Cargo Security Requirements: Final Rule required that SIDA protocols be extended to all-cargo air-operations areas at airports that offer passenger airline service and have existing SIDs. However, the rule did not require that SIDA safeguards be provided at *all* airports that serve all-cargo airline operations. This lack of consistently applied, standardized SIDA protocols negatively impacts the security of all-cargo aircraft and airline operations.

ALPA recommends that *all* airports that serve regularly scheduled all-cargo operations conducted by transport-category airliners be required to establish and maintain a designated SIDA for such operations. SIDA requirements detail perimeter security protocols, clearly define entry and exit procedures, dictate specific identification display and ramp security procedures, and are predicated on a mandatory 10-year, fingerprint-based criminal-history record check (CHRC) for all employees who maintain unescorted-access privileges within the SIDA.

Consistent application of these standards throughout the all-cargo domain would significantly enhance the security of shipments, flight crews, and parked all-cargo airliners and would greatly improve the background-screening standards needed to properly identify and vet ramp and warehouse personnel.

The Final Rule provides, in part, that: “SIDA Security measures must be extended to secured areas and air operations areas that are regularly used to load cargo on, or unload cargo from, an aircraft operated under a full program or a full all-cargo program. . . . Each airport security program will specify the limits of the cargo operations area to be included in a SIDA, subject to review and approval by TSA.”

ALPA urges the TSA and Federal Security Directors (FSDs) to apply a strict interpretation and enforcement policy related to the extension of SIDA requirements as specified in the Final Rule.

Fingerprint-Based Vetting of Persons with Unescorted Access to Cargo, Cargo Facilities, and All-Cargo Airliners

ALPA has long advocated for “One Level of Safety and Security” in regulations impacting passenger and all-cargo airline operations. Accordingly, we believe that *all* persons with unescorted access to shipments destined for transport on either passenger or all-cargo airliners



Vulnerabilities associated with name-based background checks are more easily understood when viewed in terms of the growing problem of identity theft and the potential negative consequences of misidentification.

(i.e., those who receive, inspect, transport, or load air cargo, and those with unescorted access to passenger and all-cargo airliners) must be vetted by means of a fingerprint-based (biometric) criminal-history record check. These individuals are currently subject to a biographic, name-based security threat assessment (STA), which is inadequate to determine the trustworthiness of an employee.

Currently, the fingerprint-based CHRC vetting standard is not applied to the majority of individuals who are employed in the all-cargo supply chain, many of whom are permitted unescorted access to cargo, cargo aircraft, and security-sensitive areas of airports and cargo facilities. In accordance with TSA regulations, these individuals are vetted only by means of a biographical, name-based STA, which looks for a nexus to terrorism and reviews immigration status.

The U.S. Federal Bureau of Investigation (FBI) has publicly stated that it “remains firmly opposed” to name-based background checks for non-criminal justice purposes due to the probability of inaccurate identification.¹ Name-based (non-biometric) means of identification have proved to be unreliable because of confusion related to name similarities and due to the widespread use of aliases (fictitious or assumed names) by people engaged in deceitful or criminal activity. The TSA itself has admitted, “If an individual presents fraudulent documents with an incorrect name, date of birth, country of citizenship, or other data, TSA’s STA will be flawed at inception.”²

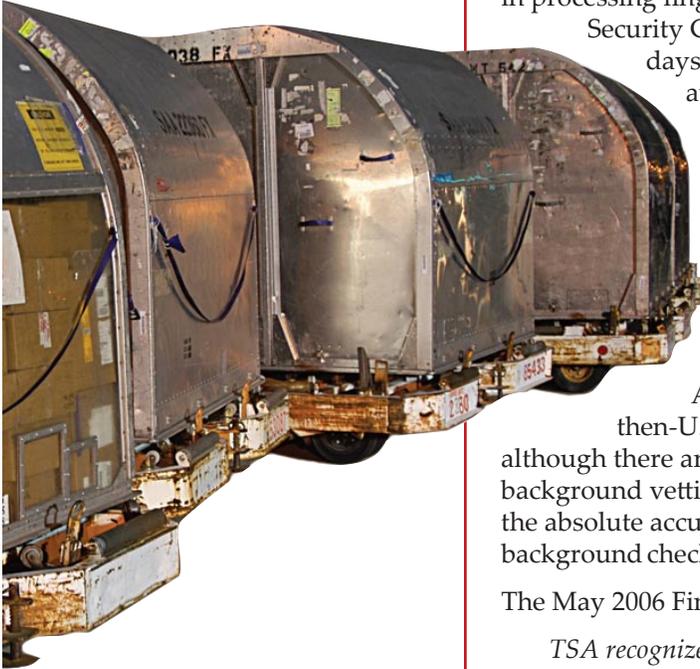
Vulnerabilities associated with name-based background checks are more easily understood when viewed in terms of the growing problem of identity theft and the potential negative consequences of misidentification. Such situations can produce either “false positive” or “false negative” results. As a consequence, some persons may be wrongfully excluded from positions for which they are qualified, or conversely, unqualified persons may be mistakenly accepted in positions for which they are unfit because of a criminal past or questionable character or financial status.

The FBI analyzed a statistically valid sample of the 6.9 million fingerprint cards submitted for employment and licensing purposes during FY1997. When compared with the criminal prints on file with the FBI, some 8.7 percent, or approximately 600,000 of the fingerprints, resulted in matches. Of greatest importance, 11.7 percent of the matches (70,200 civil fingerprint submissions) reflected names entirely different from those listed in the applicants’ criminal-history record. The FBI concluded that these persons intentionally provided false names in order to evade detection of their records of prior convictions for serious crimes and that these records were only detected because of positive, fingerprint-based identification.³

¹Testimony of David R. Loesch, assistant director in charge, Criminal Justice Information Services Division, FBI, before the House Committee on the Judiciary, Subcommittee on Crime, regarding H.R. 3410 and Name Check Efficacy (May 18, 2000).

²*Federal Register*, Docket No. TSA-2009-0018, Air Cargo Screening; Interim Final Rule.

³The Attorney General’s Report on Criminal History Background Checks (June 2006).



Without establishing the true identity and investigating the criminal history of an applicant for a job that grants unescorted access to sensitive aviation security areas, it is impossible to reliably develop a sense of the character and trustworthiness of the applicant.

Arguments defending the use of biographical rather than biometric data as the foundation of the background vetting process are often based on anticipated inconveniences resulting from perceived delays in processing fingerprint submissions. According to the Transportation Security Clearinghouse, while initially it took an average of 52 days for STA/CHRC results to be returned, currently the average response time is four hours, due to the use of better technology. As further evidence, a 1999 report issued by the U.S. Attorney General's Office states in part: "Automated fingerprint identification systems and related technologies providing for the electronic capturing and transmission of fingerprint images has made it possible to dramatically reduce fingerprint transmission and processing delays at both the state and federal levels."⁴

At a June 1997 FBI meeting in St. Petersburg, Fla., then-U.S. attorney general Janet Reno explicitly affirmed that although there are time and cost savings associated with a name-based background vetting system, its unreliability stands in stark contrast "to the absolute accuracy and reliability associated with fingerprint-based background checks."

The May 2006 Final Rule on cargo states:

TSA recognizes that there are a number of background techniques that potentially could be applied to various persons in the supply chain. In accordance with our risk based, threat managed approach, TSA has determined that requiring persons with unescorted access to cargo to submit to an STA provides a significant enhancement while limiting costs. We note that persons with more sensitive positions, such as cargo screeners, are subject to CHRCs and additional background checks.

ALPA agrees that it is prudent and necessary to conduct cost-justification calculations in determining the value of proposed security measures. In spite of the evidence indicating that biographic-based STAs do not provide the same reliable results as do biometric-based CHRCs, the decision was made to accept and utilize the STA standard. ALPA disagrees with that practice and submits that the costs associated with the realistic consequences of the hostile takeover of an all-cargo aircraft far outweigh the costs of conducting fingerprint-based CHRCs for those with unescorted access to air cargo, cargo aircraft, and cargo facilities.

There is long-established precedent for using fingerprint-based CHRCs in determining an individual's suitability for hiring. Numerous employment categories exclude convicted felons from eligibility, deeming them to be unsuitable candidates due to security concerns, character issues, and recidivism rates. Without establishing the true identity and investigating the criminal history of an applicant for a job that grants unescorted access to sensitive aviation security areas, it is impossible to reliably develop a sense of the character and trustworthiness of the applicant.

⁴Interstate Identification Index Name Check Efficacy Report of the National Task Force to the U.S. Attorney General, July 1999, NCJ-179358, www.tsa.gov/what_we_do/layers/index.shtml.

Air Cargo Security



The lack of a mandate for reinforced flight deck doors on cargo aircraft is hard to justify when the government has stated that it considers the hostile takeover of an all-cargo aircraft to be a critical risk.

Current U.S. government policies regulating the background vetting of individuals associated with the all-cargo air supply chain permit conditions in which convicted felons and others of questionable character may be granted unescorted access to cargo, cargo facilities, and cargo aircraft. These same policies permit a double standard to exist when compared to the background vetting requirements for individuals with unescorted access to cargo, cargo facilities, and aircraft in the passenger domain. This position is hard to reconcile when contemplating the government's expressed concern with "insider threats" in the aviation domain.

In order to mitigate this vulnerability, ALPA urges that the requirement for fingerprint-based CHRCs, in addition to STAs, be included in the vetting of persons who seek such employment.

Install Hardened Flight Deck Doors on All-Cargo Airliners

After September 11, 2001, the federal government required existing and future passenger airliners, but not all-cargo airliners, to be equipped with reinforced flight deck doors.

Notwithstanding this fact, some cargo airlines have voluntarily installed hardened flight deck doors on their aircraft. Today, however, a significant number of all-cargo airliners are operated in the same airspace as passenger aircraft without the benefits of hardened flight deck doors, leaving them without a way to insulate the flight deck and flight crewmembers from the airplane's interior. In fact, new wide-body cargo airplanes are being designed and built without the protections afforded by the reinforced door.

The potential for a significant lapse in security as a result of these conditions is magnified by the fact that all-cargo airliners frequently carry third-party, noncrew personnel (known as "supernumeraries"), such as couriers and animal handlers. It is also compounded by the fact that all-cargo airliners and their cargo are not protected in the same fashion as their passenger-carrying counterparts while on the ground.

The lack of a mandate for reinforced flight deck doors on cargo aircraft is hard to justify when the government has stated that it considers the hostile takeover of an all-cargo aircraft to be a critical risk. Events in the post-9/11 era have proved that stowaways represent a very real and significant threat to all-cargo airliners. All-cargo airplanes lack many of the additional layers of security identified by the TSA and TC as protecting passenger operations.⁵ This makes the need for a hardened flight deck door all the more obvious and critical.

To deter those persons with malicious intent and impede their ability to attack all-cargo flight crewmembers, gain access to aircraft controls, or otherwise execute a hostile takeover of an all-cargo airliner, physical barriers must be designed and installed to separate the all-cargo airliner's flight deck from accessible passenger and cargo areas. All-cargo

⁵ www.tsa.gov/what_we_do/layers/index.shtm.

flight decks must be clearly delineated and physically protected in the same fashion as the flight decks of passenger airliners, including the provision of reinforced flight deck doors and training for crewmembers in appropriate flight deck access procedures.

Mandated Security Training for All-Cargo Flight Crewmembers and Staff



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, must be mandated for flight crews and ground personnel supporting all-cargo flight operations. Basic and recurrent crew training must include instruction on the All-Cargo Common Strategy, and all-cargo flight crews should be provided access to TSA-issued security directives

(SDs) and information circulars (ICs) that pertain to their role as in-flight security coordinators (ISCs).

All-cargo pilots operate the same type aircraft in the same airspace as do their passenger counterparts. They frequently travel as passengers or in a deadheading status on passenger airlines. Failure to train them in the precepts of the Common Strategy not only diminishes their ability to properly secure their own aircraft and coordinate a response with other industry stakeholders when faced with threatening circumstances. It also prevents them from following industry standards when responding to a threat while traveling in the passenger domain.

Because the training guidance has already been developed by the government and provided to the all-cargo carriers, it should be made a part of the Full All-Cargo Aircraft Operator Standard Security Program, and its administration by all-cargo airlines should be mandated by the TSA, as is done in the passenger domain.

Conduct Vulnerability Assessments and Threat Mitigation

The success of any government-sponsored efforts to assess vulnerabilities within air-cargo supply-chain operations hinges upon meaningful consultation with industry subject matter experts (SMEs). Because SMEs best understand the strengths and weaknesses of their respective operational environments, they are well positioned to pro-

Because the All-Cargo Common Strategy training guidance has already been developed by the government and provided to the all-cargo carriers, the TSA should mandate it, as is done in the passenger domain.

... we continue to be challenged by an intelligent, adaptive adversary who constantly seeks ways to overcome the security measures that are intended to protect the air cargo supply chain that ultimately connects to passenger and all-cargo airliners.

vide critical insight in any attempt to find vulnerabilities contained therein and to establish effective and efficient countermeasures to potential threat vectors.

To facilitate this process, government representatives should engage air cargo SMEs in meaningful dialogue that incorporates current intelligence related to potential threats to the air-cargo supply chain.

ALPA urges all appropriate government entities to identify industry SMEs from critical disciplines within the air-cargo supply chain, solicit their input regarding the strengths and vulnerabilities within their respective operational environments, and share with them current intelligence related to threats to the cargo domain. This consultative process is necessary for government and industry partners to determine and characterize realistic threat scenarios and to develop and implement appropriate threat-mitigation practices.

Threat-Driven, Risk-Managed Approach to All-Cargo Security

In a Notice of Proposed Rulemaking (NPRM) published in the *Federal Register* on Nov. 10, 2004, the TSA proposed, among other things, to address two critical risks in the air cargo environment:

1. the hostile takeover of an all-cargo aircraft leading to its use as a weapon
2. the use of cargo to introduce an explosive device aboard a passenger aircraft.

Subsequently, in the Final Rule, the TSA articulated specific security measures intended to achieve those goals. Since that time, the majority of protective measures implemented in the all-cargo domain have been developed with the primary goal of protecting against hostile takeover.

The introduction of improvised explosive devices (IEDs) on two U.S.-flagged all-cargo aircraft in October 2010 provided evidence that we continue to be challenged by an intelligent, adaptive adversary who constantly seeks ways to overcome the security measures that are intended to protect the air-cargo supply chain that ultimately connects to passenger and all-cargo airliners.

These incidents also demonstrated that, as the threats we face in protecting the all-cargo domain from those who would do it harm continue to evolve, so, too, must the methodologies that are needed to defend against them.

In order to meet this challenge, the security measures protecting the all-cargo supply chain must mature according to a threat-driven, risk-managed methodology. Technological and procedural solutions that meet this need and accommodate the flow of commerce must be identified. ALPA recognizes that this is a difficult undertaking, but submits that failure to do so will lead to unacceptable consequences that pose a severe threat to the aviation industry in general.

... the acceptable costs associated with needed cargo-security enhancements must be measured in terms of the potential price to be paid for failing to properly protect the air-cargo industry from viable threats.



Failure to take appropriate action in this regard will expose the airline industry and the security of our nation to significant risk.

Conclusion

The disruption of an attack against the all-cargo domain in October 2010 indicates that terrorists remain interested in targeting aviation. It is significant that the attack was directed against all-cargo airplanes, because it demonstrates that intelligent, adaptive adversaries have shifted their tactics to circumvent current security measures and exploit the gaps in security standards that exist between passenger airlines and all-cargo airline operations.

While the TSA and TC, in conjunction with industry stakeholders, have done significant work to improve the security of the air-cargo supply chain, acceptable costs associated with needed cargo-security enhancements must be measured in terms of the potential price to be paid for failing to properly protect the air-cargo industry from viable threats.

Since 9/11, cash-strapped and bankrupt passenger airlines have added multiple layers of security enhancements at their own expense, while many more-profitable all-cargo air carriers have failed to keep pace in making similar improvements.

Protecting flight crews, industry personnel, passengers, and airliners engaged in or affected by air-cargo operations requires that government and industry stakeholders cooperate in achieving effective layers of security. A threat-driven, risk-based approach must be used to find and counter existing and future vulnerabilities.

While ALPA did not fully agree with the requirements of the Air Cargo Security Requirements: Final Rule, it signaled great potential for significant improvement in the security of the air-cargo supply chain. Unfortunately, implementation of a number of facets of the rule has not gone smoothly, as described previously.

ALPA commends the TSA for a number of its cargo security efforts, including increased field inspection staff and use of canine resources, research on screening technology, and research on the use of tamper-evident seals to certify the integrity of cargo shipments. ALPA urges the TSA to continue fulfilling its oversight and inspection responsibilities with respect to the security of cargo in both the passenger and all-cargo domains.

ALPA will continue to work in a collaborative spirit with its government and industry partners to identify weaknesses in the air-cargo supply chain and to encourage the development and implementation of reasonable, cost-effective solutions to those vulnerabilities. Failure to take appropriate action in this regard will expose the airline industry and the security of our nation to significant risk.