

APA and CAPA'S AVIATION SECURITY REPORT CARD

CAPTAIN JAY NORELIUS, APA SECURITY COMMITTEE, AND CHAIRMAN CAPA
CAPTAIN PAUL RANCATORE, DEPUTY CHAIRMAN, APA SECURITY COMMITTEE (2001-2004)

This article is dedicated to the memory of our fellow crewmembers, passengers, and innocent citizens who lost their lives during the murderous morning of Tuesday, September 11, 2001. It is also dedicated to you the individual crewmembers who daily remain responsible for providing safe and secure flights in our nation's aviation system.

As we go to print, security threats and events continue to unfold in a rapid vortex, including National elections, the Olympic Games and the third anniversary of 9/11. The 9/11 Commission Report, documenting far reaching governmental failures and lapses in both security and intelligence, hit the public and Congress with newfound "truth." Unlike an earlier failure to heed the "Gore Commission" report, hopefully this time the message will not fall on the deaf ears of our nation's legislators and regulatory bureaucracies.

"Highly suspicious" activities aboard our aircraft continue to remind us that each and every flight can be an opportunity for an act of terrorism or a "test run" for future attacks. Based on reports of possible Al Qaeda attacks against key financial institutions, NYC is now at "Orange Level." Moreover, in this time of a real war, both our nation and airline continue to battle for an operational balance between determined vigilance and a cultural paranoia to remain politically correct. Failure to get this right could result in our country becoming the most "PC" nation to ever become extinct. In the backdrop of these threats, every crewmember deserves our company's and nation's support as you continue to bear the responsibility for providing safe and secure flights.

Immediately following 9/11, members of the APA and CAPA Security Committee, in coordination with a multitude of other organizations, directly

impacted the language in the original Aviation Transportation Security Act (ATSA). Every APA and CAPA security committee member continues to work diligently to interface with our companies, legislators and regulators at every level to build a more secure aviation program.


CAPA's goal remains "One Level of Security" for all of commercial aircraft. Attack of the highly visible US and worldwide "free nations" aviation industry is merely a catalyst for the far reaching goal of radical terrorism. Their goal is to destroy western civilization's core infrastructure at the psychological, governmental, commercial, economic, and spiritual levels. Any aircraft (passenger or cargo), any target (people, to icons of civilization), and any means (suicide to nuclear) will be "fair game" in their sick war of destruction—therefore, one level of aviation security is the only reasonably all-inclusive defense.

INTRODUCTION TO THE AVIATION SECURITY REPORT CARD

The Aviation Security Report Card is a culmination of CAPA's efforts to assess our nation's aviation security system from an operational/pilot viewpoint. The subjects on the Report Card, while portrayed as individual grades, are best viewed as an integrated multi-layer security system. A useful analogy might be that of grading one's physician—individual grades are helpful, but it is the sum of the total physician that provides either good or bad medicine to the patient! The Report Card follows a logical operational flow: begins at the airport perimeter (includes the rising MANPAD threat), moves to the "topside" for screening, and then addresses "bottom side" inspection issues for ramp workers, vendors, contractors, caterers, etc. Credentialing and Threat Intelligence are taken as

FEATURE ARTICLE

critical pieces of preflight security. Crew training and the security layers of last resort, direct defense of the cockpit by Federal Air Marshals and Federal Flight Deck Officers close out the report card.



The Coalition of Airline Pilots Associations

AVIATION SECURITY REPORT CARD																
SUBJECT	GRADE															
PERIMETER SECURITY	D															
SCREENING	<table border="1"> <tr> <td>PEOPLE</td> <td>TOP SIDE</td> <td>C</td> <td>BOTTOM SIDE</td> <td>F</td> </tr> <tr> <td>BAGS</td> <td></td> <td>B</td> <td></td> <td></td> </tr> <tr> <td>CARGO</td> <td></td> <td></td> <td></td> <td>F</td> </tr> </table>	PEOPLE	TOP SIDE	C	BOTTOM SIDE	F	BAGS		B			CARGO				F
PEOPLE	TOP SIDE	C	BOTTOM SIDE	F												
BAGS		B														
CARGO				F												
CREDENTIALING	F															
FEDERAL AIR MARSHALS	C															
CREW TRAINING	<table border="1"> <tr> <td>ACADEMICS</td> <td>C</td> </tr> <tr> <td>SELF-DEFENSE</td> <td>F</td> </tr> </table>	ACADEMICS	C	SELF-DEFENSE	F											
ACADEMICS	C															
SELF-DEFENSE	F															
THREAT INTELLIGENCE	D															
MISSILE DEFENSE (MANPADS)	F															
PASSENGER FLIGHT DECK DOORS	B															
FEDERAL FLIGHT DECK OFFICERS	<table border="1"> <tr> <td>ACADEMICS</td> <td>D</td> </tr> <tr> <td>SELF-DEFENSE</td> <td>D</td> </tr> </table>	ACADEMICS	D	SELF-DEFENSE	D											
ACADEMICS	D															
SELF-DEFENSE	D															

"PILOTS REPRESENTING PILOTS"

PERIMETER SECURITY — GRADE "D"

Definition: The perimeter includes the area that borders the airport and AOA areas. It includes fencing, electronic surveillance, guards, and other security arrays. One unique threat is the shoulder launched anti-aircraft missile or MANPAD (discussed in a separate section).

Background: The TSA abrogates this security parameter to each individual airport authority. Little seems to be public regarding "airport perimeter standards" and the range or preparedness is a vast "unknown." ATSA language was illusive on mandates and requirements. There exist many inconsistencies in perimeter security at the different airports. Some airports are stepping up with sophisticated technology

and the use of employee biometric access systems. Unfortunately at other than the nation's most secure major airports, "chirping crickets" and broken fences remain the only perimeter defense!

Improvements are generally triggered by a breach of security. For example:

- boats penetrate a major airport's water perimeter and fishermen are found walking the perimeter road inside the airport;
- a man carrying a cylinder on his shoulder jumped the security fence in a California airport;
- stolen trucks were recently driven on taxiways and runways at another major airport.

Problems: Lack of clear congressional mandates and funding. Infighting for scarce financial resources overshadows visionary perimeter security programs. A lack of standardization, poorly defined oversight, and limited research & development programs remain in the forefront.

A Better Solution: Professional law enforcement, equipped with modern tools, and supported by technologically sound infrastructure, should be mandated and funded by Congress.

SCREENING — PEOPLE, BAGS AND CARGO — GRADES VARY

Definition: Passenger airports typically are divided logistically by two inspection areas. The upper level, top side, is where passengers and their luggage are screened prior to boarding and the lower level, bottom side, is where the aircraft are loaded with cargo and provisioned. We have broken down our grading in this area to three categories: People, Bags, and Cargo.

Background: More people are choosing to fly again. It is estimated that the summer of '04 will see an increase of passenger traffic possibly exceeding pre - 9/11 volume. At the same time, TSA will be using fewer personnel for screening with wait times exceeding two hours at some locations. In addition "privatization" of "screening" is an option beginning in Nov '04—it is unknown at this time how many airports will apply—but lack of adequate TSA staffing is a driving force in the consideration.

(continued on next page)

FEATURE ARTICLE

Grades:

“C” for People Top Side. Screening passengers improved somewhat since pre-9/11; however, newer, more capable systems are not yet incorporated that would further improve both technical issues and shorten “wait times.” A brief review of recent professional security articles reveals that technology and implementation of better and faster methods is only now beginning to move to the TSA front burner of concern. Major failing of top side people inspection system—no capability to detect non-metal explosives carried thru the “metal-only” portal detectors. Richard Reid, the AA Flight 63 “shoe bomber” with non-metal shoes and plastic explosives would still have a very reasonable chance of “getting through” the portal. Full-body scanners are used at special events (Olympics, private events, etc.) yet fall victim to the ACLU privacy issue. New “sniffer” technology is just now being tested at five domestic airports. The technology is available for much better passenger/carry-on baggage screening.

“F” for People, Bottom Side. These “people” are airline and airport employees, vendors, and contractors—for the most part they are very poorly, if at all, screened and in almost every instance, personal belongings are never inspected. Failure in employee/vendor background checks continue to be well-documented by both the GAO and in the public media. This is a known porosity which will eventually be “used against us” much as known security holes were used in the 9/11 attacks. Excuses and negative mantras abound ranging from “too expensive” or the infamous “it just can’t be done.” Sadly both the TSA and the Congress are aware and turn a blind side to the obvious — time is not on our side.

“B” for Bag screening, Top Side. Better, but primarily due to appearance and not reality. There still exists a significant variation in the consistency of explosive detection and trace capabilities — bluntly, they do not all directly detect explosives. Existing technology remains slow, cumbersome and still subject to high false positive rates with unwanted down time. The system is “people driven” which poorly utilizes scarce resources. In addition, recent GAO studies

suggest that the TSA is doing no better job than pre-9/11 in detecting and preventing passage of prohibited security items. Perhaps the grade should really be lowered to a C or C-minus. Unfortunately, another event may reveal the truth.

“F” for Cargo screening, Bottom Side. Cargo security is one of the eight areas which form an integrated aviation security system. Failure to address these together is an invitation to another disaster. Although termed “screening,” in the ATSA language, CAPA believes that “inspection” is a more realistic operational working term. Inspection of cargo on passenger carriers remains primarily a paper work drill entitled the “known shipper” program. There is a very limited amount of cargo “inspection” now taking place. Yet the inadequacies of cargo screening/inspection would never pass the topside program. One year after the ASAC reported numerous recommendations from an industry-wide Cargo Working Group, no significant cargo inspection regulations or protocol are in place. This smacks of the similar fate of the FAA “Gore Commission” following TWA 800 — much writing with no meaningful implementation. Congress, although mandated by the ATSA to provide oversight of this critical security arena, thus far remains satisfied to hold endless and ineffective “hearings.” Recently, funding for cargo security was cut and enhanced inspection was voted down and legislation requiring passenger cargo to be inspected never got to the House floor for a vote. (The current “known shipper” program propagates a multimillion dollar loss of cargo and US Mail revenue to passenger airlines — but that is a story for another *Flightline*.)

CAPA’s position is straightforward: the contents of any cargo shipped are vastly more important than who ships it. The government’s reversal of this axiom is a glaring deficiency in the nation’s aviation cargo security system.

Recent System Failures to Consider: The “Man-in-the-Box”—who shipped himself from New York to Texas—could have just as easily been shipped in the “known shipper” program. Four individuals shipped themselves in boxes “shrink-wrapped” on a cargo pallet into Miami. Even after the national aviation

FEATURE ARTICLE

threat level was raised to Orange in November 2003, the TSA allowed a waiver for palletized and shrink-wrapped cargo. In another system breach, an employee shipped bomb parts to himself via cargo carrier from California. Today, little inspection is done for “walk-in” boxes dropped off at cargo carrier locations.

Planned Improvements Remain Nearly Invisible: Successful technology screening/inspection for cargo does exist at various overseas locations. Yet, only in April 2004 did the TSA finally publish a Request for Information (RFI) for a national level review of technological improvements for cargo inspection methods and hardware. However, at the July 2004 DHS Technology Symposium there was no mention of aviation cargo security research & development programs. Several government agencies are on record as stating that a cargo aircraft explosion would only kill a few pilots. They fail to understand the potential use of cargo aircraft as a weapon of mass destruction. In July, a new GAO report evaluating aviation cargo security was commissioned by various congressional committees. APA and CAPA members who served on the TSA “Cargo Working Groups” were interviewed by the GAO and their dissenting opinions thoroughly discussed.

CREDENTIALING—GRADE OF “F”

Definition: Aircraft security demands that proper identification be mandated for anyone with access to the cockpit — aircrew, armed Law Enforcement Officers (LEOs), FAA/TSA Inspectors all fall into this critical “know who is really on board” category.

Background: An effective biometric ID protocol for all LEOs was funded, tested and approved to be implemented on September 11, 2001. Yet the TSA elected to “start over” with a massive nationwide credentialing effort entitled the Transportation Worker Identification Card (TWIC). The TWIC was envisioned to “cover” millions of workers at hundreds of airports, harbors, trucking terminals, and even bus stations nationwide.

TWIC’s Future: Dismal at best—there were 20 pilot programs planned in 2003, a few now in place only cover seaports, NO aviation. Most likely an additional 18-24 month funding pushback—\$67 million allocated for FY 2004 limited to pilot projects and consultant fees—no FY 2005 funding. System is no

longer seen as access control—only a secure ID system. However, there are effective programs in place at a variety of other governmental agencies and individual airports—just not for aircraft security. Worse, current industry experts predict a useable TWIC systems to be “years” away.

A Glimmer of Hope: The TSA Registered Traveler “test” program is underway and crewmembers are allowed to participate (AA is using BOS and DCA). This may be a “beginning point” for a separate crew biometric ID program—time will tell.

FEDERAL AIR MARSHAL PROGRAM — GRADE “C” BUT MAY BE DROPPING!

Definition: Federal Air Marshals (FAMs) enforce federal laws onboard commercial aircraft, including laws relating to acts of terrorism, hijacking, or aircraft piracy and laws relating to violent, abusive, or disruptive behavior by passengers in air transportation.

Background: The FAM program has been in existence for some time and was stepped up significantly after 9/11.

Grade “C” and dropping! CAPA members have the greatest respect for our Federal Air Marshals but they are limited in numbers, and accordingly, can only cover a limited number of flights. The international community remains a ‘limited player’ for the FAM program. Funding was just cut for FY 2005, the “last” FAM was recently trained and future hiring is currently “frozen.” None of these are good signs for the FAM program.

CREW TRAINING

Definition: We break down crew training into academic and self-defense training. Academic training refers to the class work crewmembers undergo during recurrent training cycles. Self-defense training is the hands-on instruction received to counter terrorist threats.

Background: Academic curriculum has been updated since 9/11 to reflect lessons learned. Crew self-defense training has been studied to determine whether it should be mandated or not.

Grades:

“C” for Academic Training. The training aircrews receive varies widely from airline to airline due to lack of standardization. TSA (*continued on next page*)

FEATURE ARTICLE

just released a 2004 revision to the Common Strategy and mandatory Training Standards with no effective input from “stakeholders” or the industry. The outcome of the TSA’s “solo” only approach to security training may well be another loser.

“F” for Self-Defense Training. There are no established standards for training. Programs vary from “some” to “none” airline-to-airline. Recently, following national flight attendant outrage, the TSA is resurrecting the so-called “advanced” self-defense training. But, Congress caved to airline pressure and allowed this debacle of voluntary attendance at no cost to the airlines. Issues from “who will really attend on their days off,” “who pays” and “who is libel for injuries in voluntary training” remain unanswered.

THREAT INTELLIGENCE—GRADE “D”

Definition: Receiving timely reports on suspicious activity and known operational threat information are obvious requirements to conduct a safe and secure flight. This concept should extend to “proactive” knowledge of the types of suspicious activity for crewmembers to watch for as well as “follow up” lessons learned after events occur.

Background: The Captain, by federal regulation, is the in-flight security coordinator and needs to receive the most current threat intelligence reports before departure. Yet, to date, TSA does not mandate that Security Directives (SDs), Information Circulars (ICs), suspicious activity, etc., be provided to crewmembers. Most corporate security offices fail to provide this information—American and Southwest Airlines are the exceptions. In addition the various national aviation security agencies—DHS, TSA, FAMS—have failed to establish proactive distribution systems for lessons learned from suspicious events and/or information provided to the Joint Terrorism Task Force.

Planned Improvements: There are indications that the TSA may take a more positive stance to ensure that airline Captains receive the most current Intel updates before they fly. Recently the TSA Administrator suggested to the president of the ATA that he contact ATA’s members and consider using the AA distribution methods as a model. Problem: ATA is a lobbying organization not devoted to security issues and many US passenger and cargo airlines are not members of ATA. The TSA should simply

MANDATE the distribution of critical SDs and ICs.

MISSILE DEFENSE — SO FAR AN “F”

Definition: Surface-to-air missiles, especially the man portable heat-seeking missiles (MANPADS), are a proven threat to commercial aircraft.

Background: Shoulder-fired heat-seeking missiles date back to the Vietnam war. Since then the technology incorporated in these missiles has improved substantially. Recently, a DHL cargo Airbus was hit by a heat-seeking missile and, fortunately, landed back at Baghdad Int’l Airport. Military aircraft carry countermeasure equipment to defeat this threat; commercial aircraft do not. Recently El AL announced equipping their aircraft with MANPAD countermeasures—FAA currently requires those countermeasures to be “turned off” in US airspace! NOTE: Both DHS and TSA spokesmen contend that MANPADS do not pose a credible threat to domestic aviation. While CAPA sincerely hopes DHS and TSA are right, it will only take one MANPAD fired at a US carrier to bring the US aviation industry crashing down.

Why Failing Grade: Currently, commercial aircraft are not equipped with any MANPAD countermeasure equipment. Congress shows interest, some funds allocated for research & development and DHS is now on a two-year “fast track” timeline for testing. (American is participating with one of the contractors in the program.) August should see the completion of ongoing research & development testing for three competing systems with the possible selection of one, more or even none as the recommended defense systems. However, any recommendations will remain a long way from implementation with unknown program cost and questionable outcomes.

PASSENGER FLIGHT DECK DOORS—GRADE “B”

Definition: A door that separates the passenger compartment and the cockpit equipped with a lockable device that can be unlocked only from inside the flight deck.

Background: Reduces—but does not totally deny—unauthorized persons gaining access to the flight deck of a commercial aircraft.

Why Grade: “B” The reinforced doors are installed and appear to be working well. There remain some technical problems associated (*continued on page 17*)

FEATURE

(continued from page 9)

with system failure, deadbolts, and MEL issues. CAPA recommended to the original RRT and for the ATSA legislation that “double” door type barriers be mandated. CAPA still maintains that position as a better solution to the total cockpit access issue. It remains noteworthy that many cargo aircraft do not even have cockpit doors and those that do are not required to have hardened doors. Hence the grade of “F” for cargo security. In addition, international carriers are not mandated to install hardened doors.

FEDERAL FLIGHT DECK OFFICERS — GRADE OF DOUBLE “D”

Definition: Program to authorize pilots to carry firearms on their possession during flight to ensure the protection of passengers and safe conduct of flight.

Background: Only a small minority of pilots have volunteered because of the cumbersome constraints of application process, personal costs (both \$\$\$ and using days off) and remote training facility. Both APA and CAPA have dedicated committees dealing with FFDO issues.

Planned Improvements: S.2268 and H.R. 4126 “The Cockpit Security Technical Corrections and Improvements Act of 2004” address issues that will allow the FFDO program to function as it was originally intended. For more information see page 24.

SUMMARY

This is not a very “pretty” report card and the American public should be concerned with the known porosity in the system. Another terrorist attack similar to 9/11 will devastate the nation’s aviation system. On the other hand, the Report Card points to a myriad of opportunities for Congress, the DHS, and the TSA to improve aviation security. CAPA is deeply committed to working closely with the administration and Congress to field the best aviation security system possible. Our goal remains to reduce the success rate for terrorism from 100% to near zero—absolute zero would be best, but in a free society with some degree of system porosity “zero” will be very difficult to obtain. We must implement changes within our control that increase security and enhance commerce—those goals are not mutually exclusive if done properly. 