



U.S. House of Representatives
Committee on Transportation and Infrastructure

Washington, DC 20515

John L. Mica
Chairman

Nick J. Rahall, III
Ranking Member

James W. Coon II, Chief of Staff

April 11, 2011

James H. Zoia, Democrat Chief of Staff

MEMORANDUM

TO: Members, Transportation & Infrastructure Committee

FROM: John L. Mica, Chairman

SUBJECT: Oversight and Investigations hearing on the use of biometric credentials for airline pilots and other transportation workers, Thursday, April 14 at 9 a.m. in room 2253 RHOB

PURPOSE

The Full Committee will meet on Thursday, April 14, 2011, at 9:00 a.m. to receive testimony from the Federal Aviation Administration (FAA), the Transportation Security Administration (TSA), and the National Institute of Standards and Technology (NIST). The hearing will focus on efforts made by FAA and TSA to provide biometric credentials to airline pilots and other transportation workers, as well as the NIST standard for these credentials.

BACKGROUND

In 2003 the White House issued Homeland Security Presidential Directive – 7 (the Directive), establishing a national policy for Federal departments and agencies to “identify and prioritize critical infrastructure (CI) and to protect them from terrorist attack.”¹ The Directive identifies the roles various agencies have in securing CI and directs the Secretary of Homeland Security to work closely with other Federal departments and agencies to achieve the goals established in the Directive. In addition to the coordination responsibilities granted to the Department of Homeland Security (DHS), the Directive makes certain components of the Executive Office of the President accountable for functions related to the protection of CI relevant to their sector.

¹“Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection,” The White House (December 17, 2003)

As it relates to the Department of Transportation (DOT), the Directive states: “The Department of Transportation and the Department (of Homeland Security) will collaborate on all matters relating to transportation security and transportation infrastructure protection.”

The U.S. transportation network is essential to our way of life and economic vitality. The open nature of the transportation network and our dependence on it make it a prime target for terrorist attack. Evidence of terrorist intent to attack modes of transportation can be seen in the Madrid train bombings of 2004 and 2006; the London train and bus bombings in 2004; the liquid explosive bomb plot in 2006; the attempt to detonate a fuel system at JFK International Airport in 2007; the Christmas Day attempt to blow up a flight from Amsterdam to Detroit in 2009; and the 2010 Yemeni plot to disguise bombs as printer cartridges on cargo planes destined to Chicago.

It is impossible to completely secure every mode of transportation from terrorist attack. To do so would cost untold billions of dollars and disrupt commerce. Since 9/11, Congress has advocated for a more risk-based and cost-effective approach through the issuance of biometric credentials for those individuals that have already been vetted by the Federal government. These credentials can be used to expedite screening at airports for cleared individuals, allowing scarce resources to be redirected toward those individuals that may pose a risk. Biometric credentials are also used to verify the identity of employees with access to secure areas of the Nation’s critical infrastructure, ensuring that those that intend to do harm are not able to disguise themselves in such a way that would grant them unchallenged access to secure areas.

This memo discusses the guidance that the White House and Legislative Branch has issued to Federal departments and agencies since 9/11 to begin issuing biometric credentials to cleared transportation workers and to develop expedited screening programs for airline pilots, airport workers, and other individuals with unescorted access to secure areas designated in vessel or facility security plans; and the Administration’s progress in fulfilling these mandates.

GUIDING DOCUMENTS

- ***Aviation and Transportation Security Act (2001), P.L. 107-21***
This Act authorized TSA to provide for the use of biometric or other technology that positively verifies the identity of each employee and law enforcement officer who enters a secure area of an airport, but subsequently amended to require that TSA issue guidance for the use of such biometric or other technology not later than March 31, 2005. This Act required TSA to work with airport operators to strengthen access control points in secured areas to ensure the security of passengers and aircraft and consider the deployment of biometric or similar technologies that identify individuals based on unique personal characteristics.

The Act also required TSA to establish pilot programs in at least 20 airports to test and evaluate new and emerging technology for providing access control and other security protections for closed or secure areas of the airports, and may include biometric or other technology that ensures only authorized access to secured areas.

In addition, the Act required TSA to conduct an assessment that reviews, among other things, the effectiveness of biometrics systems that were in use at U.S. airports. After the assessment, TSA was to recommend to airport operators commercially available measures or procedures to prevent access to secure airport areas by unauthorized persons.

- ***National Strategy for Homeland Security (2002)***²
The first White House National Strategy for Homeland Security warned that finding terrorists and preventing terrorist attacks in the United States is difficult because false documents and simple disguises can allow a terrorist on the FBI's Watch List to sneak past security personnel at an airport. The Department of Homeland Security called for additional research and development in biometric technology to address this challenge.
- ***Maritime and Transportation Security Act of 2002, P.L. 107-295***
This Act required the Secretary of Homeland Security to issue a biometric transportation security card to individuals with unescorted access to a secure area designated in a vessel or facility security plan.
- ***Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection (2003)***
HSPD-7 directed the Secretary of Homeland Security to produce a comprehensive, integrated National Plan for Critical Infrastructure and Key Resources Protection including a strategy to identify, prioritize, and coordinate the protection of critical infrastructure and key resources. The Directive mandates the DOT and the Department of Homeland Security (DHS) to collaborate on all matters relating to transportation security and transportation infrastructure protection.
- ***Intelligence Reform and Terrorism Prevention Act of 2004, P.L. 108-458***
Sec. 4022 Improved Pilot Licenses
This Act mandated that not later than one year after the date of enactment, the Administrator of the FAA must begin to issue improved pilot licenses consistent with the requirements of title 49, United States Code, and title 14, Code of Federal Regulations. The Act further specified the improved pilots licenses would be resistant to tampering, alteration, and counterfeiting; include a photograph of the individual to whom the license is issued; and be capable of accommodating a digital photograph, a biometric identifier, or any other unique identifier that the Administrator considered necessary.
- ***Security and Accountability for Every Port (SAFE Port) Act of 2006, P.L. 109-347***
This Act codified into law a transportation security card program (the Transportation Worker Identification Credential "TWIC" program) and required the program to be implemented at all U.S. ports not later than January 1, 2009.

² "National Strategy for Homeland Security," The Office of Homeland Security (July 2002)

- ***Implementing the Recommendations of the 9/11 Act of 2007, P.L. 110-53***
Sec. 1614 Security Credentials for Airline Crews
 The Administrator of the TSA, after consultation with airline, airport, and flight crew representatives, must submit a report to Congress on the status of the Administration's efforts to institute a sterile area access system or method that will enhance security by properly identifying authorized airline flight deck and cabin crew members at screening checkpoints and granting them expedited access through screening checkpoints. The Administrator must begin implementation of the system or method not later than one year after the date on which the Administrator submits the report (or February 2009).

- ***National Strategy for Homeland Security (2007)***³
 The 2007 White House National Strategy for Homeland Security warned that terrorists may seek to infiltrate or recruit an individual with privileged access to a hardened site. The Strategy also cautioned that insiders can offer terrorist enemies information on exploitable vulnerabilities or provide terrorist operatives access to sensitive or controlled areas.

TRANSPORTATION WORKER IDENTIFICATION CREDENTIAL

Section 70103(c) of title 46 of the United States Code requires the owners or operators of vessels or maritime transportation facilities to prepare vessel and facility security plans. These plans must include provisions that establish and control access to secure areas on the vessel or at the facility. Section 70105 requires individuals entering secure areas designated in a security plan to either hold a "biometric transportation security card" or be accompanied by someone with such a card. The section directs the Secretary of Homeland Security to issue cards. It also lists disqualifying offenses, establishes a waiver procedure, and an appeals process for individuals who are denied waivers.

DHS implemented this requirement through the creation of the Transportation Worker identification Credential (TWIC). TWICs contain a fingerprint, but not a retina scan. As of March 31, 2011:

- 1,699,373 TWICs have been activated;
- 86,069 initial disqualification letters had been issued;
- 44,477 appeals requested;
- 43,326 appeals granted;
- 8,219 waivers requested;
- 7,495 waivers granted;
- 54 appeals requested; and
- 1,158 final disqualification letters issued.

The TWIC requirement was enacted in 2002. TSA began issuing cards in October 2007. Cards have now been issued to workers at all ports where cards are required and to all

³ "National Strategy for Homeland Security," The Homeland Security Council (October 2007)

U.S. mariners. TWICs are valid for five years so the renewal process will begin in the next year. The cards costs \$132.50, and the program is required to be fully paid for by fees.

The SAFE PORT ACT of 2006 also established a deadline of April 2009 to issue final rules for the deployment of TWIC readers. However, TSA is still conducting the pilot program and has informed Congress they do not expect to issue final rules for the readers until late 2012. Without biometric readers in place, the biometric identification function is not being used when granting access to secure areas.

Additionally, the recently enacted Coast Guard Authorization Act clarifies that mariners who work aboard vessels that are **not** required to file vessel security plans (mostly small passenger vessels) are **not** required to have a TWIC. Despite this change in law, TSA and the United States Coast Guard continue to require TWICs for all merchant mariners whether or not they require access to secure areas.

BIOMETRICS FOR PILOT LICENSES

Section 4022 of the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 directed the Administrator of the FAA to begin issuing improved pilot licenses consistent with the requirements of title 49, United States Code, and title 14, Code of Federal Regulations. IRTPA mandated that within one year after enactment, or by December 17, 2005, FAA must begin issuing improved pilots licenses that:

1. are resistant to tampering, alteration, and counterfeiting;
2. include a photograph of the individual to whom the license is issued; and
3. are capable of accommodating a digital photograph, a biometric identifier, or any other unique identifier that the Administrator considers necessary.

Six years later, FAA still has not included biometric identifiers or photographs on pilot licenses. Once the photograph mandate is implemented, a pilot license will be an acceptable identification card to use at airport checkpoints and, according to existing Federal standards for personal identity verification cards, a pilot license may be used to quickly and electronically verify pilot identification at airport checkpoints, allowing pilots to bypass physical screening.

AIRLINE CREW SCREENING PROGRAMS

The Implementing the 9/11 Recommendations Act of 2007 mandated the Administrator of TSA to begin implementation of a sterile area access system that will “enhance security by properly identifying authorized airline flight deck and cabin crew members at screening checkpoints and granting them expedited access through screening checkpoints.”⁴ The Administrator had 540 days from the date of enactment, or by February of 2009, to begin implementation of this system.

⁴ Public Law 110-53, august 3, 2007

In February of 2007 the Air Line Pilots Association convened an industry working group to develop a proposal to meet this mandate. Their resulting proposal, called Crew Personnel Advanced Screening System (CrewPASS), was based on the Cockpit Access Security System (CASS).

CASS provided a system to verify the identification of airline crew seeking jumpseat access privileges on other airlines' aircrafts. Riding in the cockpit jumpseat allowed airline crew the ability to position for flight assignments. Further, this program permitted gate agents to verify the identity of flight crew members by using a secure, Internet-based interface to transmit a photograph of the crew member along with background information and credentials. CASS was field tested in 2003 and fully operational by the end of 2005.

CrewPASS

CrewPASS leveraged the CASS database to validate the identity of flight crew members at exit lanes and allow them access to sterile areas in the airport. Testing for this program began in July of 2008 at Baltimore-Washington International Airport, Pittsburg International Airport, and Columbia Metropolitan Airport and was limited to uniformed flight crew members and did not include biometric credentials.

SecureScreen

From September 17, 2008 through November 23 2008, a separate pilot program operated at the Baltimore Washington International Airport with the Southwest Airlines Pilots' Association called "SecureScreen." This pilot program included biometric authentication of pilot identities through fingerprints and digital photographs. Throughout the length of the pilot program, 213 Southwest Airline pilots enrolled to participate, and there was a 99.78 percent success rate for user authentication and approved access authority. The enrolled pilots provided favorable feedback, and TSA acknowledged the success of the program.

Guidelines for Expanded Pilot Program for Expedited Access to Airport Sterile Areas for Crewmembers (TSA, Transportation Sector Network Management)

In June of 2009 TSA issued guidelines for an expedited access system to sterile areas of airports for properly credentialed commercial flight deck and cabin crewmembers. The program specifications and requirements included real-time employment verification, photo identification, and biometric verification of all participating crewmembers.

SecureCrew

On November 19, 2010 American Airlines (AA) submitted a request to TSA to implement a biometric crew access system at Dallas-Fort Worth International Airport in accordance with the above-referenced TSA guidelines called "SecureCrew." This program was in accordance with TSA guidelines and jointly sponsored by the International Air Transport Association. Upon receipt of AA's request, TSA asked questions related to interoperability and scale and AA informed TSA that the SecureCrew system was both

interoperable and could be used by other airlines as a nationwide solution. The system would utilize two forms of a biometrics: a fingerprint and a digital photograph. TSA did not approve this pilot program.

KnownCrewMember

In November of 2010, TSA Administrator Pistole announced his intent to expand the program nationwide. TSA announced its intent to roll out a 90-day pilot program called "Known Crew Member" at seven airports later this year.⁵

The program will allow airline pilots to present their airline identification to a TSA agent in the exit lane or other approved area in an airport in order to verify identity and allow an expedited screening process. As intended for the initial seven airports, KnownCrewMember will not utilize biometric identifiers as directed in its June 2009 guidance.

The use of airline IDs for the purpose of verifying identity also has several flaws. Airline IDs are not federally-issued, do not comply with federal standards for personal identity verification, and are issued by multiple airlines resulting in the lack of a cohesive and interoperable standard.

AIRPORT WORKER SCREENER PROGRAMS

More than 600,000 airport workers have access to secure areas of airports every day.⁶ It is the policy of most airports to allow airport workers to bypass physical screening in exchange for identification checks and random screening programs. Bi-partisan congressional concern over this practice has existed for years, with opponents noting that this practice creates vulnerabilities where individuals with stolen or counterfeit identification can access secure areas of the airport.

In 2007 a Comair employee smuggled 13 semiautomatic handguns, a rifle, and eight pounds of marijuana in a carry-on bag on a Delta Airlines flight from Orlando, Florida to San Juan, Puerto Rico. The employee was able to smuggle these items onboard because his access credentials allowed him to bypass passenger screening checkpoints.

Various programs have been implemented across the nation to ensure that that secure areas of airports are protected, however a uniform standard for biometric credentials and access control programs for airport workers has yet to be established.

⁵ Chicago O'Hare, Detroit Metro, Phoenix Sky Harbor, Boston Logan, Miami International, Dulles International and Seattle-Tacoma

⁶ "Airport Passenger Screening: Background and Issues for Congress," Congressional Research Service: Bart Elias, Specialist in Aviation Policy (April 23, 2009)

FEDERAL STANDARD FOR PERSONAL IDENTITY CREDENTIALS

On August 27, 2004 the White House issued HSPD – 12 directing a common identification standard for federal employees and contractors. HSPD – 12 says:

Wide variations in the quality and security of forms of identification used to gain access to secure Federal and other facilities where there is potential for terrorist attacks need to be eliminated. Therefore, it is the policy of the United States to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors.⁷

Such forms of identification must be (a) issued based on sound criteria for verifying an individual employee's identity; (b) strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; (c) rapidly authenticated electronically; and (d) issued only by providers whose reliability has been established by an official accreditation process.

HSPD-12 directs the Secretary of Commerce to promulgate a Federal standard for secure and reliable forms of identification in consultation with the Secretary of state, the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, the Director of the Office of Management and Budget, and the Director of the Office of Science and Technology Policy.

In compliance with the HSPD-12, the Department of Commerce, through NIST, issued FIPS-201 for Personal Identity Verification (PIV) in March of 2006. This standard provides the technical framework for including biometrics in identification cards for Federal employees and contractors (these cards are commonly known as "PIV Cards").

Special Publication (SP) 800-76-1 was issued in 2007 to provide the technical details for PIV cards, and SP 800-76-2 is due this year and will revise the standard to include new iris biometric and match-on-card⁸ technology.

PERSONAL IDENTITY VERIFICATION – INTEROPABLE (PIV-I)

Although non-federal organizations are unable to fully comply with FIPS-201 standards because there are some requirements that can only be met by the Federal Government, such as the sponsorship of a Federal department or agency, there is a desire within the non-federal community to issue identity cards that are (a) technically interoperable with Federal government PIV systems, and (b) issued in a manner that allows Federal government relying parties to trust the cards.⁹

⁷ HSPD-12, August 27, 2004

⁸ Match-on-card technology both matches and stores fingerprints on a Smart Card.

⁹ Personal Identity Verification Interoperability for Non-Federal Issuers, Federal CIO Council May 2009

In May of 2009 the Federal Chief Information Officers Council issued a set of minimum requirements to align non-federally issued identity cards to the FIPS-201 standard called PIV-I. Private sector entities that do business with the Federal government, such as defense contractors, often issue PIV-I access cards to employees. This ensures that government employers may be confident that information and resources related to contracted programs is secured in a manner equal to what is done in the Federal government.

In addition, there are federally sponsored programs that may issue identity cards to non-federal issuers. Examples of these programs include the First Responder Authentication Credential, Transportation Worker Identity Credential, and Airport Credential Interoperability Solution. In these instances the program is sponsored by the Federal government but the recipients of identity cards are not Federal employees or contractors.

The PIV-I standard is used in these cases to ensure interoperability and technical compatibility with the federal PIV standard. TWIC is aligned with PIV-I standards, and it is also the standard that would apply to the inclusion of biometric identifiers on pilot licenses.

WITNESSES

The Committee will hear testimony from the following witnesses:

The Honorable John Pistole

Administrator

Transportation Security Administration

Mr. John Schwartz

TWIC Program Manager

Transportation Security Administration

Ms. Peggy Gilligan

Associate Administrator for Aviation Safety

Federal Aviation Administration

Ms. Cita Furlani

Director, Information Technology Laboratory

National Institute of Standards and Technology