BIOMETRIC IDs FOR PILOTS AND TRANSPORTATION WORKERS: DIARY OF FAILURES

(112–26)

HEARING

BEFORE THE

COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

APRIL 14, 2011

Printed for the use of the
Committee on Transportation and Infrastructure

Available online at: http://www.gpo.gov/fdsys/browse/committee.action?chamber=house&committee=transportation

U.S. GOVERNMENT PRINTING OFFICE

65–851 PDF WASHINGTON : 2011

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE

JOHN L. MICA, Florida, *Chairman*

DON YOUNG, Alaska
THOMAS E. PETRI, Wisconsin
HOWARD COBLE, North Carolina
JOHN J. DUNCAN, JR., Tennessee
FRANK A. LOBIONDO, New Jersey
GARY G. MILLER, California
TIMOTHY V. JOHNSON, Illinois
SAM GRAVES, Missouri
BILL SHUSTER, Pennsylvania
SHELLEY MOORE CAPITO, West Virginia
JEAN SCHMIDT, Ohio
CANDICE S. MILLER, Michigan
DUNCAN HUNTER, California
ANDY HARRIS, Maryland
ERIC A. "RICK" CRAWFORD, Arkansas
JAIME HERRERA BEUTLER, Washington
FRANK C. GUINTA, New Hampshire
RANDY HULTGREN, Illinois
LOU BARLETTA, Pennsylvania
CHIP CRAVAACK, Minnesota
BLAKE FARENTHOLD, Texas
LARRY BUCSHON, Indiana
BILLY LONG, Missouri
BOB GIBBS, Ohio
PATRICK MEEHAN, Pennsylvania
RICHARD L. HANNA, New York
STEPHEN LEE FINCHER, Tennessee
JEFFREY M. LANDRY, Louisiana
STEVE SOUTHERLAND II, Florida
JEFF DENHAM, California
JAMES LANKFORD, Oklahoma
VACANCY

NICK J. RAHALL II, West Virginia
PETER A. DEFAZIO, Oregon
JERRY F. COSTELLO, Illinois
ELEANOR HOLMES NORTON, District of Columbia
JERROLD NADLER, New York
CORRINE BROWN, Florida
BOB FILNER, California
EDDIE BERNICE JOHNSON, Texas
ELIJAH E. CUMMINGS, Maryland
LEONARD L. BOSWELL, Iowa
TIM HOLDEN, Pennsylvania
RICK LARSEN, Washington
MICHAEL E. CAPUANO, Massachusetts
TIMOTHY H. BISHOP, New York
MICHAEL H. MICHAUD, Maine
RUSS CARNAHAN, Missouri
GRACE F. NAPOLITANO, California
DANIEL LIPINSKI, Illinois
MAZIE K. HIRONO, Hawaii
JASON ALTMIRE, Pennsylvania
TIMOTHY J. WALZ, Minnesota
HEATH SHULER, North Carolina
STEVE COHEN, Tennessee
LAURA RICHARDSON, California
ALBIO SIRES, New Jersey
DONNA F. EDWARDS, Maryland

CONTENTS

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

John L. Mica
Chairman

Washington, DC 20515

Nick J. Rahall, II
Ranking Member

James W. Coon II, Chief of Staff

James H. Zoia, Democrat Chief of Staff

April 11, 2011

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. 107-71*
  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-referencedTSA 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-card[8] 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

BIOMETRIC IDs FOR PILOTS AND TRANSPORTATION WORKERS: DIARY OF FAILURES

THURSDAY, APRIL 14, 2011

HOUSE OF REPRESENTATIVES,
COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE,
WASHINGTON, DC.

The committee met, pursuant to notice, at 9:30 a.m. in Room 2253, Rayburn House Office Building, Hon. John L. Mica (Chairman of the committee) presiding.

Mr. MICA. I would like to call this hearing of the House Transportation and Infrastructure Committee to order this morning. I welcome you. This is an Oversight and Investigations hearing that will focus on the issue of the use of biometric credentials for airline pilots and other transportation workers. And this is, again, part of our investigations and oversight of our committee, and being handled this morning at the full committee level. And I appreciate the participation of other Members this morning. I think we will be joined by a few more. There are conflicting schedules; I apologize for the delay in beginning this. We had our governor in town, so we ended up with a triple booking this morning, and I appreciate everyone's courtesy in allowing us to start a little bit late this morning.

The topic and—the order of business will be opening statements by Members, and then we will go to our witnesses. And if anyone would like to submit comments or additional information to the record, without objection that will be so ordered.

Again, the purpose for us being here this morning is to review the progress and sometimes the lack of progress in producing a pilot's license that has both information that identifies the pilot in a manner that we prescribed some time ago—I think 6 or 7 years ago—by law. At that particular juncture, when we found the pilot's license looked like it sort of came out of a Cracker Jack box, it was just a little folded piece of paper, could easily be duplicated, we passed a law that said we should have a biometric measure, we should have a photograph, and that we should have a durable identification card. That was enacted by law some time ago, and we still don't have that particular card available.

Do we have a copy of one of the—may I? If you want to bring that up here, and maybe just put it in front, this is what we have ended up with, is—here, let me just take this, here. You can see, again, the only pilots that are on the license that has been produced at millions of taxpayer dollars, the only pilots on the license that is now in use is—happened to be Wilbur and Orville Wright.

And the back of this particular license has a metallic strip. And, unfortunately, it does not have the biometric capability that we asked for in law.

So, they spent millions of dollars in producing this pilot's license that, again, does not meet what we believe is required by law, and does not provide us with identification. And although we do not have anyone from TSA here today to testify, in fact, TSA will not accept this as an identification card.

What is even more disturbing is we spent about $420 million, we will be approaching half-a-billion dollars on producing a transportation worker identification card. We have passed in law requirements on a number of occasions, and I believe at least four times into Federal law, the production of a transportation identification card that would have a biometric measure, capable of having several measures, both thumbprint, iris, and then also, of course, a photograph of the transportation worker.

Having spent nearly a half-a-billion dollars on this, we have produced a card. They have been distributed. We do have biometric capability, we do have a photograph. However, we do not have a reader, and we have yet to establish a standard or agree on a standard for a biometric measure of iris.

So, in both of the programs, while the pilot license is almost a complete disaster, what concerns me is that TSA has now embarked on two programs, one in, I think, 2007—one was a crew access program, and—creating several pilot programs working, I think probably with good intentions, with some of the pilot associations. But in 2007 they worked on CrewPASS and in 2010 the administrator announced his intent to expand a new program, and that is Known Crewmember, to seven airports at the end of last year.

So, we have a pilot's license that TSA will not accept as identification, it doesn't meet the criteria set forth in law. We have a transportation worker—and we spent millions of dollars on that—we have a transportation worker identification card which is in use now, but we don't have the use or acceptable reader, nor do we have iris standard developed. So, that is where we find ourselves.

I am disappointed that TSA again has declined this committee's invitation to testify on their action and their current work in developing a biometric crewmember credential and pilot's license. I don't believe that the industry should be responsible for setting a standard or developing a pass that should be—that would be used and would be acceptable. I believe that is clearly the responsibility of the Federal Government, and something that we have attempted to do by law.

Now, since TSA has decided not to show up here today, I have consulted with the chairman of the Homeland Security Committee and also with an investigative panel on which I also serve, and I can assure you that we will have TSA testifying, either at a joint future hearing with one of those two committees to, again, try to get some responsiveness from an agency that, for some reason, does not want to respond, nor participate in developing an identification card, both for transportation workers or for pilots or for the many individuals who are involved in transportation work and do so in a cost-effective and timely manner.

So, that is where we find ourselves today. Very disappointed. A huge amount of taxpayer money has been expended. You would think that we could also have some better response from the agency that is primarily charged with this.

Come on in, Mr. Farenthold. We can put Members right up here, too. We are a little squeezed for space today, but those arriving a little bit late will get the front row. We haven't used this hearing room too much because, again, the size of the committee. But we have—every bit of space in the Capitol that we, I think, the Transportation and Infrastructure Committee, has available is being used today.

Mr. Boswell, come up and join us up here. And staff is welcome to just put a chair up here. I want to make sure all of our Members are accommodated.

But again, I thank the Members for joining us today. I wish it could be under different circumstances, and we could have the cooperation of TSA, but we do not have it today. But we will get it in the future, as I said, one way or the other.

With that, I would like to recognize any other Members for opening statements. Mr. Long? Mr. Cravaack?

Mr. CRAVAACK. Thank you, Mr. Chairman, and thank you for all the people that have come out today. This is a very important issue, and kind of near and dear to my heart, so I appreciate you coming here today.

I would like to welcome the witnesses on our panel. I look forward to hearing your testimony regarding the FAA and TSA's biometric transportation credential efforts. I am very disappointed that TSA is not here today. I had some very pointed questions that I wanted to ask them, and I am very disappointed they are—for them not being here today.

As you know, the United States transportation system remains a target and a means through which the terrorists seek to attack our homeland. I appreciate your efforts taken in the wake of 9/11 to protect our transportation system from attack. A number of bills have been enacted to direct a cost-effective, risk-based approach in protecting our credentialing system.

To date, a number of our statutory directives requiring the issuance of biometric credentials have not been implemented, or have been partially implemented. To me, this is very disappointing.

I look forward to hearing from our witnesses about what is presently being done to comply with the law, and why there has been such a delay to this point. I thank you again, and I look forward to hearing your testimony, and I yield back, sir.

Mr. MICA. Thank you. And I would like to recognize any other Members that may have opening statements. You are recognized, Mr. Landry.

Mr. LANDRY. Thank you. It is good to be so close to you all.

[Laughter.]

Mr. LANDRY. I thank the Chairman for calling this hearing today. I certainly want to ensure that our transportation system is as secure as possible. Every day our transportation system moves more than 1.4 million shipments of hazardous materials, any of which could potentially be used to harm Americans. Securing all

this cargo is daunting. No one doubts that fact. But it is also achievable.

Unfortunately, some of our security interests—security entities have lost sight of an important part of the transportation security system feasibility. I wish that the Transportation Security Administration had accepted our invitation to come to today's hearing, because they need to hear this. Right now, TSA is worried about their own feasibility, what is easiest for them. I think that TSA needs to worry more about what is feasible for the worker.

To me, TSA's requirement that a worker—for a worker to make two visits to the TWIC enrollment center, one to enroll for their TWIC card and another to pick up the card is the definition of an unnecessary burden. Now, I know that TSA has said that a TWIC card must meet the FIPS 201 standard, and must be in the worker's possession at all times, and I know that the soon-to-be-released GAO report will probably say that mailing is not an option, but what about other solutions? Are we honestly telling transportation workers, "Sorry, guys, your government has thought long and hard about this situation and the entire universe of possible solutions we have been able to brainstorm, and all we can come up with is to get"—I am sorry—"we have been able to brainstorm is you come to get the card or we mail it to you, and our accountant tells us that the last one is no good," meaning mailing it to you.

Come on. We are all smart people here. We can figure out a way that the worker does not have to make a second trip just to pick up the card. For some TWIC workers, this means a trip of hundreds of miles, and they have to make this trip twice. We need to do better than that.

I also have another issue with the TWIC card. Recently a company in my district got in trouble with DHS because they did not have I–9's on file for all of its employees, even though the company had a record of all of these employees' driver's licenses, birth certificates, Coast Guard licenses, and a TWIC card. Considering the fact that everyone would have to have—considering the fact that everything one would have to have to secure a TWIC card is at least that stringent, if not more stringent, than the information one needs to secure an I–9, can't we change the law to ensure that a TWIC card can serve as an I–9, thereby lessening the paperwork that companies such as the one in my district are required to comply with?

Again, I wish that the TSA were here to address these issues, but I do not know—but I do know they are watching this hearing. So I just wanted to put them on notice about the concerns on the TWIC card.

Thank you, Mr. Chairman.

Mr. MICA. Thank you. Any other Members seek recognition?

[No response.]

Mr. MICA. Well, again, the order of business will be we will turn to our witnesses. And, as you can see, Mr. Pistole has the—the administrator of TSA—has refused to appear. It also concerns me that Mr. John Schwartz, who is the TWIC program manager, transportation worker identification credential program manager of—and he is with the Department of Homeland Security—has also refused to appear before the committee today.

For those Members who have joined us just lately, we are consulting with both the Homeland Security Committee, Oversight and Government Reform Investigative Committee, and we will have them appear one way or the other, either in a joint hearing or through the other committees. Because, again, I thought it was not unreasonable for us to ask them to comment on this.

And since they now are involved in two pilot—have been involved in two pilot programs to develop pilot licenses and—or identification cards that they would be using in lieu of a pilot's license, and we are producing a pilot's license at great public cost, I thought the least that they could do is come and provide us with a status of both of those programs: TWIC, which is the transportation worker identification card; and the pilot's license issue.

We also tried to meet with them behind closed doors. The intent of the committee's work is not to embarrass any agency. And we did conduct a meeting. Some of you participated in that behind closed doors. And we, unfortunately, had the same response and unwillingness to work with the committee from TSA. So I can say to all the Members they are not building a very good strong warm, fuzzy relationship in their effort to assist us.

And I know they have been distracted this week. If you just watch television and—you see the current issues of an agency that is struggling to gain control of itself and its important security mission.

So with that being said, we are pleased to have two witnesses this morning who can shed some highlights and review with the committee the progress both of the pilot's license, which was mandated by law, prescribed by law to FAA, and they had undertaken that mission with some difficulty, as we learned in both the closed door meeting, and we will hear more about today. So we have Peggy Gilligan, who is associate administrator for the—for aviation security of FAA. And Ms. Cita Furlani, the director of Information Technology Laboratory of the National Institute of Standards and Technology, who sets some of the standards that are required for these identification documents.

So, with that, maybe we could—I could recognize first Ms. Gilligan, and you could give us sort of a history of the problems we have encountered with the pilot's license and also the status of where we are going from here.

So, welcome, and you are recognized.

TESTIMONY OF MARGARET GILLIGAN, ASSOCIATE ADMINISTRATOR FOR AVIATION SAFETY, FEDERAL AVIATION ADMINISTRATION; AND CITA M. FURLANI, DIRECTOR, INFORMATION TECHNOLOGY LABORATORY, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, DEPARTMENT OF COMMERCE

Ms. GILLIGAN. Thank you, Mr. Chairman. Thank you, Chairman Mica, Congressman Rahall, and members of the committee. I want to thank you for the opportunity to appear before you today on the issue of embedding biometric identifiers on pilot certificates.

I know that this issue has been of significant interest to you, Mr. Chairman, because, as you mentioned, we have had several meetings on the topic. In these meetings, it has been clear that FAA has

not acted as directed by this committee, not as quickly nor as comprehensively as intended. But I would like to outline what FAA has done in the area, and how we intend to move forward.

The purpose of the pilot certificate for many years was simply to document that the holder met the required aeronautical knowledge and experience standards to fly an airplane. For decades, paper certificates worked effectively for that intended purpose.

Starting in the late 1980s, law enforcement agencies, with mandates other than aviation safety, began to see potential misuse of pilot certificates as they engaged in activities related to the war against drugs. In 1988, the Drug Enforcement Assistance Act required FAA to phase out paper certificates and replace them with tamper-resistant certificates. As of April 2010, all pilots have received enhanced plastic certificates. Those certificates were at a cost of $2.7 million for all of the 700,000 pilots that we have in our registry. We continue to replace certificates for mechanics, dispatchers, and other certificate holders, and those will be completed by March of 2013.

Mr. Chairman, I know you question the value of our new certificates, but I can assure you that the colors, holograms, and even the images of Orville and Wilbur Wright have made it very difficult for our new certificates to be forged.

After the tragic events of September 11, 2001, with aviation playing such a central role in the disaster, additional risks were identified for pilot certificates. In October 2002, we required all pilots to carry a government-issued photo ID any time they were exercising their pilot privileges. This way, any FAA inspector who asked for pilot credentials, and every fixed-base operator who leased an aircraft, could confirm the person's identity, as well as their qualifications to fly.

The Intelligence Reform and Terrorism Prevention Act of 2004 imposed additional requirements on the certificate, beyond just being tamper-resistant. It called for a photograph and that it be capable of accommodating a digital photo or other biometric identifiers. We did not act right away. We did not act quickly. Without any experience in the area of——

Mr. MICA. If I could interrupt the witness for just a second, some of the Members came in late, and Mr. Boswell just gave us his pilot's license. And, as you just heard the witness testify, Congress required that there be a photo on the ID, a biometric measure, and it be durable. Well, the license that was produced actually meets one of those requirements. It is durable. The only pilots to appear on the license that was issued—and this is Mr. Boswell—is Wilbur and Orville Wright. And although I guess he looks a little bit like Wilbur——

[Laughter.]

Mr. MICA. This is the ID that millions of dollars has produced. And the biometric strip, or the metallic strip here, does not have the biometric capability that was required in law.

So, thank you for loaning us this. And it is Exhibit A. We had another one here, but you can see what was issued. Yes, yes, that was a bigger one. But this is the real one. And thank you, Mr. Boswell, for handing that to the Chair.

And I apologize for interrupting, but it does show what has been produced. You may continue.

Ms. GILLIGAN. Thank you, sir. Without any experience, or expertise in the area of biometrics, we understood that other government agencies such as NIST were developing biometric standards. And at that time the newly formed Transportation Security Administration was looking at what would be the appropriate identifiers for transportation workers. We were hopeful not to duplicate or otherwise interfere with those efforts and, in fact, to take advantage of them.

After waiting far too long, in November of 2010 we issued a notice of proposed rulemaking that proposed to require that all pilots, including student pilots, possess certificates with a digital photo, which is generally considered to be a biometric identifier. The comment period for that rulemaking closed in February.

Due to the broad scope and the economic impact of the rule on over 700,000 certificated pilots, we proposed to phase in the requirement over a 5-year period. FAA recognizes that this timeframe is not consistent with the act's direction, which called for us to begin modifying certificates in 2005. But we are working hard to finalize that rulemaking.

While we proposed the requirement for the digital photo, we didn't know what other type of biometric information to include on the certificate, or how to set up the infrastructure to collect and protect fingerprints or other biometric data from 700,000 pilots. So we did not move forward, as the committee expected.

We all support the goal of enhancing aviation security and maximizing resources in order to achieve a single, universal security credential, incorporating biometric data that meets common standards. To meet this goal we will continue to work with TSA on its proposal to establish a universal ID for transportation workers.

We need to understand how best to move forward to improve the use of biometric data to ensure the security of the pilot community and enhance aviation security. This requires coordination among government agencies and cooperation with airlines, industry trade associations, and aviation labor organizations. We recognize the advantages of developing security-enhancing uses for airmen biometrics, and we look forward to working with this committee as our efforts progress.

Mr. Chairman, I will take whatever questions.

Mr. MICA. Thank you. And we will hold questions. We have got another witness that we want to hear from first, and that is the director of the information technology laboratory, at the National Institute of Standards and Technology, who helped develop some of those standards and requirements for these identification documents, and that is Cita Furlani.

Welcome, and you are recognized.

Ms. FURLANI. Thank you, Chairman Mica and Ranking Member Rahall and members of the committee. I am Cita Furlani, director of the Information Technology Laboratory at the Department of Commerce's National Institute of Standards and Technology. Thank you for the opportunity to appear before you today to discuss our role in standards and testing for biometrics and identity management.

NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards and technology in ways that enhance economic security and improve our quality of life.

Founded in 1901, NIST is a non-regulatory Federal agency. We have more than four decades of experience in improving the quality, usability, and consistency of human identification systems, responding to government and market requirements. We perform research and collaborate with other Federal agencies, academia, and industry partners to support timely development of biometric standards and to develop required conformance testing architectures and testing tools.

NIST has developed standards to support Federal agencies' information security requirements for many years beginning in the early 1970s, with the enactment of the Brooks Act. Through the Federal Information Security Management Act, or FISMA, of 2002, Congress reaffirmed this leadership role in developing standards for cyber security. FISMA provides for the development and promulgation of Federal Information Processing Standards, or FIPS, that are compulsory and binding for Federal computer systems other than national security systems.

The responsibility for the development of FIPS rests with NIST. The authority to promulgate mandatory FIPS is given to the Secretary of Commerce. NIST develops FIPS when there are compelling Federal Government requirements such as for security and interoperability and there are no acceptable industry standards or solutions.

To satisfy the requirements of Homeland Security Presidential Directive 12, NIST developed FIPS 201, entitled, "Personal Identity Verification," or PIV, "of Federal Employees and Contractors." It was approved by the Secretary of Commerce and issued in 2005. 6.2 million cards that comply with FIPS 201 have been issued to Federal employees and contractors. In addition, the Department of Defense Common Access Cards are conformant.

FIPS 201 incorporates in NIST Special Publication 800–76, which describes technical specifications for the biometric credentials of the PIV system, including the PIV card itself. This document is currently being updated to include optional use of compact iris image records, with iris records required in the absence of fingerprints. This update is an important step forward in the use of biometric data for PIV.

NIST is engaging the public in the development and review of this document, which is expected to be released soon for public comment. Under the provisions of the National Technology Transfer and Advancement Act, and OMB Circular A–119, NIST is tasked with the role of encouraging and coordinating Federal agency use of voluntary consensus standards, and participation in the development of such relevant standards.

In fact, United States-led international efforts have produced standards publicly adopted by the European community and by Australia. We continue to work with these standards committees to ensure compatibility with Federal credentials, and to address the needs of non-Federal communities.

Conformance testing to biometric standards measures whether a product's implementation faithfully implements the specification. NIST actively contributes to the development of these conformance testing methodologies. The usability and ease of use of biometric systems is an overarching need for deployed biometric systems within the Federal Government. We have applied our expertise in usability and biometrics to study biometric systems in border security and airport environments.

With NIST's extensive experience and broad array of expertise both in its laboratories and its successful collaborations with the private sector and other government agencies, we are actively pursuing the standards and measurement research necessary to deploy reliable, usable, interoperable, and secure identity management systems.

Thank you for the opportunity to testify today on NIST's activities in biometrics and identity management. I would be happy to answer any questions you may have.

Mr. MICA. Well, thank you, and I thank both of our witnesses. We are, again, disappointed that TSA would not show up.

We are right now engaged in producing a transportation worker identification card and making certain it is properly deployed, and also involved in creating a credential for pilots that would be used instead of current pilot's licenses for identification, since the pilot's license that we now have is not acceptable to TSA.

Let me just ask Peggy Gilligan, who is with FAA and overseeing aviation security and documentation for the pilots, if that is, in fact, the case, do you know that TSA will accept the pilot's license for identification purposes that you have produced?

Ms. GILLIGAN. You are correct, sir. It is not used as an identification method at this point. Again, as I testified——

Mr. MICA. Because it does not have a photograph. Is that—I guess that is the principle reason.

Ms. GILLIGAN. I would assume so. Again, right now, the certificate demonstrates what your qualifications are, as a pilot, which is historically the reason that we issued it. We issued it so that we would know that, in fact, someone was competent and qualified to fly an airplane.

Certainly, as we look at the biometric requirements, it may be able to fill the role of an identification card, and that is part of what we are coordinating with TSA. We want to assure we don't have a proliferation of identification cards, to your point, sir.

Mr. MICA. How much have we spent on the program so far?

Ms. GILLIGAN. For the FAA licenses?

Mr. MICA. Yes.

Ms. GILLIGAN. It has cost us about $2.7 million to replace all of the pilot certificates, and we have about 700,000 active pilots.

Mr. MICA. And are they all—have all of the pilots received the new license now?

Ms. GILLIGAN. As of April 2010, this month, they will have completed that. Yes, sir.

Mr. MICA. And the reason for not having either the biometric standard or—well, the photograph would be sort of a simple thing. Was there any reason that they didn't include the photograph as, I thought we directed fairly clearly by law? Is there any reason for

not having the—at least the pilot's photograph, instead of Wilbur and Orville?

Ms. GILLIGAN. Yes, sir. When we began the program to replace the certificates with the plastic tamper-proof certificates, that was in response to a different legislative direction that we had received earlier. That process was already underway, and we allowed that to go forward and it was completed.

We have now, as you know—and I will acknowledge and take responsibility for being way too late in the process—but we have now proposed to require digital photographs, as well as to try to develop a process for the 700,000 pilots to be able to provide those photographs in a convenient way around——

Mr. MICA. How long will it be, and how much is—is that going to be another $2.7 million to also get out new—or is it going to cost more or less?

Ms. GILLIGAN. The notice of proposed rulemaking has already been out for comment. The comment period has closed. And so now we are considering the comments from the pilots about the program. We will issue the final rule within about a year, and then we will set a timeframe for that replacement process. Because, again, there are——

Mr. MICA. So it will be a year before you establish the rule, and then you start replacing those cards after that. And what is the estimated cost?

Ms. GILLIGAN. We had proposed a 5-year time period for completely replacing all of the pilot certificates. We will consider that time period as we go to the final rule. That may change. And I apologize, sir, I don't have the number off the top of my head. The notice of proposed rulemaking did have the proposed cost, or——

Mr. MICA. So that would take us——

Ms. GILLIGAN [continuing]. The anticipated cost. I can provide that.

Mr. MICA [continuing]. To 2012 before we get a decision on which way we are going, and with what kind of card. And then it will take us another 5 years to get the new cards out, and I am sure at least another 2.7—2017, that would be about a decade to get the cards out, as they should be produced.

Ms. GILLIGAN. I understand your frustration, sir.

Mr. MICA. OK.

Ms. GILLIGAN. But we do have a community of 700,000 pilots. It will take a while for us to be able to replace those certificates.

Mr. MICA. And finally, when you do the card—now the standards have been in place for some time. At least for part of the biometric measure, which is the fingerprint, and also the information and data arranged in an order set by the—what do you call it, NIST——

Ms. GILLIGAN. NIST.

Mr. MICA. National Institute of Standards and Technology. I should say the whole thing, so people know what we are talking about. But they have, in fact, set the standards. Other agencies have adopted the cards.

When we did our little roundtable behind closed doors we saw the cards that most of the other agencies have produced. What prompted some of this, Members, is we also have received a Coast

Guard—one of the Coast Guard officers showed me his identification card, which is in compliance with the standards that have been set, and has incredible capabilities, including computer access from anywhere, and is encoded with, again, all of the information that is necessary for that individual, both for identification and then for certain types of access. But those standards are available. And the new card, I would imagine, would meet those standards. And it would have a photograph.

And just a final question to Ms. Furlani. The biometric standard for iris, that is still in progress. And while we have some readers, we have 1.5 million TWIC cards that have been issued, but we really don't have readers that are being used on a regular basis. Some, I learned, were approved, but they are not being used. So, we have identification card, which has part of the biometrics.

Your—so it is a twofold question, two-part question. When will you finish the iris capability? And then, when would we have a reader that could actually be used and employ both iris, fingerprint, and of course, it would have the photo?

Ms. FURLANI. The iris standard will be—the draft publication will be published in the next—very soon, within days.

Mr. MICA. In the next very soon?

[Laughter.]

Ms. FURLANI. Well, hopefully before next week.

Mr. MICA. All right.

Ms. FURLANI. But it is in progress. And what that is, of course, has been worked with the industry partners who do develop the cameras that collect the iris information. And one reason that the standard will be so readily adopted is because there are many vendors producing those cameras. So they are available, and they will agree with—be able to use the standard.

Mr. MICA. And when would this standard be issued?

Ms. FURLANI. In about—well, we put it out for public comment, we review all those comments, and if there are significant changes that come in, then we would put out a second draft. So it is over a period of months, but it is to be——

Mr. MICA. By the end of the year?

Ms. FURLANI. Oh, yes, yes.

Mr. MICA. Oh, yes. OK. So we will have a card that we have asked for by law, or—and standards for identification card. I think we have asked for it at least four times in law, various legislation, some time this year. And we will have all those requirements and a standard. And you will also be adopting those standards, Ms. Gilligan, for FAA for the pilot's license.

Ms. GILLIGAN. Yes, sir. We certainly look at those. Again, I think the infrastructure necessary to use——

Mr. MICA. OK. Well, that might be a—Mr.—we have a vice chairman of the aviation subcommittee, may be in conference. We could be very specific about what they should do, at least adopting the standards.

And when we held this behind-closed-doors meeting, we had all the agencies and DOD and others, except for TSA and Homeland Security, of course, but—and even the House Sergeant at Arms, because we thought it would be good for House Members to have a card that also incorporates the standards that have been adapted

to. It would just—I think it would make sense. Sometimes, you know, I have these wild ideas.

But again, let me yield to other Members. Let me go—Mr. Cravaack, our vice chairman, and then we will go to other Members for questions. You are recognized.

Mr. CRAVAACK. Thank you, Mr. Chairman. And, once again, thank you for coming here today on a pretty important issue, actually, from my perspective.

One of the things I am kind of concerned about is TSA. And I wish—again, I wish that TSA was here today. But their new program, Known Crewmember, is the FAA aware of this program? Were they able to discuss with you what their intentions were, and what were your thoughts on that?

Ms. GILLIGAN. I am aware of the program, I have talked with some of the representatives from the Air Line Pilots Association who were involved in it, as well as the Air Transport Association. So I am familiar with the effort, which is an effort to allow crewmembers to pass through security perhaps a little more quickly, because of the known nature of their need to be at the airport and inside the secure area.

Mr. CRAVAACK. Right. And all they are doing is using their airline ID, correct?

Ms. GILLIGAN. That is correct.

Mr. CRAVAACK. To go through. And that is the only source of identification?

Ms. GILLIGAN. As I understand it, they are going to use the airline ID, the employee ID number, and have access to a computer base that will confirm that that number is associated with the individual presenting the card.

Mr. CRAVAACK. OK. So they do back it up, via——

Ms. GILLIGAN. My understanding is that that is what it will be. I don't know where they are in the pilot programs.

Mr. CRAVAACK. Yes. One of the things I just caution is that sometimes, you know, in not-too-distant history, in a FedEx incident where there was a disgruntled employee that got access to a jump seat in a cockpit, took the crew axe out and butchered the pilots. So we want to make sure that that obviously does not occur.

And with that said, I do applaud trying to expedite crewmembers—and I would say crewmembers including all flight crew—getting through these systems. But it does take a—by the way, Mr. Chairman, I do like the card of Orville. I thought it was a very nice card, by the way, it is very nicely done.

Ms. GILLIGAN. Thank you.

Mr. CRAVAACK. And—but I do think that we do need an expedited process of getting flight crews through there, because I remember going through and them pulling tweezers out of my bag when I had a huge crash axe right behind me and quite a large aircraft that I could have done a lot of things with.

So, you know, being able to trust pilots is essential. But with that said, we have to have very updated data to make sure that there is not any pilots or crewmembers that would be trying to infiltrate the system, you know, by somebody—somebody had an action against them, had their ID pulled, or used some other ID to get through. That is what concerns me the most. And I think bio-

metric devices like a retina scan or something like that would be very good in this process, and give a lot of faith and confidence to the public, as we go through. So, I appreciate that.

What is it—in regards to your knowledge with the—sir, I don't have a counter on here, I don't want to take too much time, but I do not see——

Mr. MICA. No, we do not have a counter today, but just to——

Mr. CRAVAACK. OK. Good.

Mr. MICA. Try to share the time.

Mr. CRAVAACK. OK, thank you. To your knowledge, did TSA consider a biometric pilot license instead of airline IDs prior to this?

Ms. GILLIGAN. We have had ongoing and longstanding conversations with TSA on exactly what should be the way to identify pilots—in this case, and transportation workers, generally. And I know the Chairman shares a concern about a proliferation of identification——

Mr. CRAVAACK. Right.

Ms. GILLIGAN [continuing]. Cards for different purposes. But we have not been very successful in drawing those conversations to a conclusion. And I know that is the source of the Chairman's frustration. But we will continue to work that.

Mr. CRAVAACK. And if I could just offer a suggestion, I think the airlines themselves would be more than happy to partner with you, because we all had IDs with pictures on them. So you have a source of—and those have to be—I can't remember how many years they had to be updated, so I am sure that they could partner with you, as well.

And I don't want to take too much time here, so—but thank you very much, again, for coming. I do appreciate it. Again, I wish we had had other members—the TSA—because I think it would be a very good conversation to have. And, Mr. Chairman, I yield back. Thank you.

Mr. MICA. Thank you.

Ms. GILLIGAN. Thank you.

Mr. MICA. Other Members for questions? Mr. Hanna?

Mr. HANNA. Ms. Gilligan, I am a private pilot, an amateur pilot, but I spend a lot of time flying. And I just had my license redone about a year ago and it cost me $2 to get Orville and his brother's photograph on my card.

I thought at the time—and I know a lot of—I know hundreds of pilots spend a lot of time around airports. They are kind of like the bars for people who don't drink, you know, they are real great places to hang out.

[Laughter.]

Ms. GILLIGAN. I am glad to hear they don't drink.

Mr. HANNA. No, they don't. No. That is one thing pilots don't do is drink. It is—it really works better that way.

Ms. GILLIGAN. Yes.

[Laughter.]

Mr. HANNA. The—my point is it cost me $2 to get my license replaced. You spent $2 million. You could have easily charged me $5 and had it cost you nothing.

And you also stated that it took you 2 years to cycle through 750,000 people, one of which was me. It seems to me then, if that

is the case, why should it take a year to do something you know ultimately you are going to have to do? And why should it take, beyond that, another 5 years to do it? Because I can assure you there are no pilots who are against this. If there is anybody who wants security at airports, it is pilots, since, you know, they are busy when they are flying and the last thing they need is trouble behind them.

It seems like—based on your own experience and what you have been able to accomplish in the past, it seems like a long time.

Ms. GILLIGAN. I understand that, sir. This is one of a number of rulemakings we have underway. We have another half-dozen rules which were directed by this committee last summer with very short timeframes. So part of this is a resource issue at FAA. But we will continue and finalize the rule.

Unfortunately, there are some pilots who do not necessarily agree with this. We got about 400 comments suggesting that there are lots of other ways pilots have identification, and they do not consider their pilot certificate should be used for identification purposes. They use their pilot's license for a different reason. So, we will have to work our way through those comments and make sure we are balancing the concerns identified.

Then we have the dilemma of how to collect photos, and make sure that the person giving us the photo is the person whose certificate we want to issue. So we are looking at the infrastructure of where will pilots have to go to be able to bring us their photos or provide us the digital photos. So there are some logistical issues involved with it, as well, all of which we are working through as we finalize the rule.

Mr. CRAVAACK. Would you yield for a question?

Mr. HANNA. Oh, sure.

Mr. CRAVAACK. My—one of the questions I have is who is—who actually needs the pilot's license with a picture on it? Usually only those flying in a commercial status. So all pilots, not necessarily, would need to have a picture or biometric devices associated with their pilot's license, only those working, for example, that would have to have access to a secure area. Don't you think?

To be honest with you, for a security measure, only those individuals would truly need to have the type of identification that you are talking about. So not all pilots—not all 700,000 pilots—need to have this type of identification.

Ms. GILLIGAN. Well, the committee direction does require all pilots. And, in addition, at the time, during the debate, there was discussion about the potential security risk of general aviation aircraft, and the idea that FBOs should be able to properly identify people to whom they are leasing aircraft. That these pilots would have somehow been vetted.

Now, of course—and I probably should have mentioned this because some of the new Members may not know—the entire airman registry is vetted through TSA and through other law enforcement organizations regularly. It is now vetted 24 hours a day, 7 days a week, 365 days a year, in an effort to identify any known risk or threat from someone who may hold one of our certificates. And if we are notified by TSA that there is a risk, we revoke certificates based on the TSA determination of a security risk.

So, we have addressed that sort of known risk when we are able to identify it. So that is ongoing. But right now the legislation does anticipate all pilots would, in fact, get the new certificates with photographs and biometrics.

Mr. CRAVAACK. I will have to educate myself more on that. Thank you very much, and I yield back, sir. Thank you.

Ms. GILLIGAN. Sir, we will be glad to come and talk with you any time to let you know what we have done and where we are going. Thank you.

Mr. MICA. OK. Mr. Hanna, were you finished?

Mr. HANNA. Do you happen to know AOPA's position on this? Have they rendered one?

Ms. GILLIGAN. They have. I am sure they commented, sir. I don't recall.

But I agree with you. Fundamentally, there is not a lot of disagreement.

Mr. HANNA. I use a number of different airports, so I carry a lot of cards.

Ms. GILLIGAN. Yes.

Mr. HANNA. So, for what little it matters, I would like one.

Ms. GILLIGAN. Absolutely. And the Chairman has made that point, as well.

Mr. MICA. Well, if the gentleman will yield——

Mr. HANNA. Yes.

Mr. MICA. You know they do have—TSA does have several programs. They started one in 2007. Now we are on another one in 2010 to produce credentials. But I don't believe it is the role of the Air Line Pilots Association, the commercial airliners, to produce identification that should be acceptable by TSA or acceptable as a pilot's—in lieu of a pilot's license. So, while we are producing a pilot's license already, why not have that capability?

And the standards also that the National Institute is setting, the type of card—and embedded in it you can have encodement for all kinds of different levels of access. So—but if we had—well, if we had true biometric measures of both iris and thumbprint, and a photo, we would have a triple check that that individual is that individual, that we have an honest documentation that they have access to certain levels of activities. And again, we are not producing a whole host of identifications that go on and on, nor is the—a private company setting the standard that is acceptable.

So, that is where we are. And I don't care if AOPA or any of the others or the airlines like it. They can all go fly in a different direction. But we will make certain—I can assure you, as sure as we are at this hearing today in this room, that we will have this matter resolved in the FAA legislation that will pass Congress very shortly. So this is an important area.

Mr. Bucshon, you have been waiting, and then we will go to Mr. Farenthold.

Dr. BUCSHON. Thank you, Mr. Chairman. I appreciate it. I am not an aviation person. Unlike some of the others, I was a physician prior to coming here.

But I want to make a few general comments about government, and why I am here, and this is a classic example, I think, of why the American people are disgruntled with the Federal Government.

In my view, I mean, the Congress has given directed orders to fix a problem that seems fairly simple. And I suspect most major private security firms could have solved this problem years ago. But the Federal Government continues to blame everybody, you know. Not having TSA here gives the people who are here plausible deniability that, well, it is the TSA's fault, and the TSA is going to say it is your fault. And I just want to say that this is one of the reasons why the American people want this government to change.

You know, you commented on 400 comments that you received from the public on this issue out of 700,000 pilots that would be affected like this. And in medicine I would call that something that is called anecdote, which is—I know you needed to consider it, but statistically, this is an extremely small number of concerns for a problem that affects the entire American aviation system.

So, I would like to know, Ms. Gilligan, what are the real reasons why we cannot fix this problem? Just cut through all the blaming of the agencies, cut through all of the politics. How come a problem that I think the private sector could have solved in a matter of months, literally, has taken years, and how come people can continue to say—even though Congress has directed this to happen, just come here and tell us that—and blame other people, and tell us why you have not done it?

So, I want to know—I really want to know. What is the real reason why we cannot fix this?

Ms. GILLIGAN. Yes, sir. In part, it is because we did not step up to do it in a timely way. In part, it is because FAA has no experience in biometrics or how to collect them or how to keep them and protect them——

Dr. BUCSHON. I am going to interrupt, just for a second.

Ms. GILLIGAN. Yes, sir.

Dr. BUCSHON. There are many private companies around this Nation, I can tell you, that are experts at this. And this could have been solved, I mean, within weeks.

You know, we do not have to reinvent the wheel every time something comes up. There is no reason why the FAA needs to be an expert in biometrics. There is private companies and other agencies within the government that are experts in this area. So I do not think that—that is not a valid excuse.

Ms. GILLIGAN. It is not meant by way of excuse, sir. It is simply part of the facts. We did reach out to TSA, because they also had direction, as the Chairman has indicated, to establish biometric indicators for all transportation workers, including pilots. And we felt it would be appropriate to follow their lead. That lead has not led us to a conclusion. And so we are continuing to work the issue.

I understand your frustration. I agree, this could have been done sooner and quicker. But we are where we are at this point, and we are working hard to try to move forward.

Dr. BUCSHON. But it has been how many years, approximately, since you were directed to do this that it has not been done?

Ms. GILLIGAN. The direction, I believe, was in 2004.

Dr. BUCSHON. 2004. That is 7 years. I mean in anyone's mind in the American public that are watching this hearing, they would say

that that is a ridiculous amount of time to solve this problem. And so——

Mr. MICA. Will the gentleman yield?

Dr. BUCSHON. I will yield.

Mr. MICA. I mean what you have learned today is it is 7 years to date, and we have got another year to go before we get the comments, and then 5 years to deploy. So we are looking at more than a decade to, again, solve a relatively—well, it is not a simple requirement that Congress has set forth, but if you are frustrated, Mr. Bucshon, I have been here for the whole thing, so——

[Laughter.]

Mr. MICA. I am at the end of my wits on it. I yield back.

Dr. BUCSHON. And I do not—I am not—and there is no disrespect here among what you are trying to do, of course. But I think I am passing on the frustration of the American people, not only for this issue, but many others.

And so, I really—I mean it is an honest question. What is the real reason why we cannot do this?

Ms. GILLIGAN. Again, I think we looked for expertise from others, which has not been forthcoming. And the reality that is—putting in place an infrastructure to collect and protect biometrics for 700,000 pilots is a somewhat daunting task.

So, at FAA we have the identification cards, as many agencies do. We have about 70,000 employees. We set up 170 collection locations. For 10 times that number of pilots, the infrastructure needed to collect and protect this data is something that really needs to be carefully constructed. And we had hoped to draw on the expertise of others who do this, and we have not successfully completed that.

Dr. BUCSHON. OK, thank you. I yield back.

Mr. MICA. Mr. Farenthold?

Mr. FARENTHOLD. Thank you very much, Mr. Chairman. And I agree. I am stunned at how long this process took. I walked in here, they took my picture and had a photo ID for me in a matter of 5 minutes when I became a freshman here that had holograms on it and was tamper resistant. You can walk into any amusement park in the country, buy a season pass, and they will put your picture on it. You know, in—OK, it probably takes longer than 5 minutes; he has got to wait in line to get it. So, I mean, I am just stunned by this.

Let's talk a little bit more about the detailed biometrics. Ms. Furlani, how much data does it take to store appropriate amount of biometric data on a card? I mean is it a kilobyte? Is it a megabyte? I mean just give me an order of——

Ms. FURLANI. I do not have those numbers, but that is the challenge. You have put your finger on it. And that is one of the reasons it has been difficult on the iris—and it is only recently we found a way to reduce the amount of data that needs to be stored on the card that permits it to move into the standard. So it is——

Mr. FARENTHOLD. So we are talking about something that probably cannot be stored on a magnetic strip, it is going to require——

Ms. FURLANI. Oh, it needs a——

Mr. FARENTHOLD [continuing]. An embedded chip, or something like——

Ms. FURLANI. With encryption. You need to have the encryption to protect it.

Mr. FARENTHOLD. OK. Now, I assume also that you have got to have some way of telling whether or not that ID has been revoked or not. So it is going to be online. So, really, do you really need that much data? Can't you just store a serial number, have the user know a PIN, and it looks it up online at the same time it looks to see if it has been revoked?

Ms. FURLANI. You want all the intelligence on the cards, and that is what is the protective device. And you do need the PIN to identify that you are the person——

Mr. FARENTHOLD. Right. I mean I get—something you have, something you know, something you are.

Ms. FURLANI. You got it.

Mr. FARENTHOLD. But it seems to me there is going to have to be an online component to that anyway, to check revocation.

Ms. FURLANI. Correct. And that is what—when you have the readers, that is what they do, is confirm that there is a validity. And, as the Chairman said, what actual access each individual should have.

Mr. FARENTHOLD. OK——

Ms. FURLANI. Because that could be controlled through the——

Mr. FARENTHOLD. So, I mean, the technology is there. Clear had the cards that they embedded it on them. OK, admittedly, they went out of business. But, you know, they did not have the Federal Government behind them.

Ms. FURLANI. Well, it is a business model.

Mr. FARENTHOLD. Yes. You have got—CBP has something similar, their trusted entry program that I know of. American Express blue cards have a chip embedded in them. They cannot be that expensive.

Ms. FURLANI. Correct. And the reason they are not expensive, and are available, are the basic standards and the interoperability, so vendors can compete and build better products, and thus enter the market more acceptably. So——

Mr. FARENTHOLD. OK. So it is not expensive. We get the standards out. We ought to just be able to get this done in a short amount of time. Texas changed their driver's license—what is it, over 10 million drivers in Texas—in a matter of—you know, as soon as they all expired, all changed. Done.

So, again, I am troubled by—and I am also troubled, Ms. Gilligan, you are talking about, well, how do we collect the pictures of the pilot. We ask our TWIC longshoremen to appear in person twice to have their picture taken. If anybody ought to be able to get around to a location easily, it ought to be a pilot. You know, they can fly to wherever you want.

I mean, admittedly, I realize that is an exaggeration. I mean if you are in the middle of, you know, some rural area, it is potentially a long trip there. But I cannot believe that with a—the hardware to make these ID cards costs more than a couple of thousand dollars with just a picture. Obviously, a little bit more with the biometric data.

Can you explain why pilots—we are asking less of our pilots than we are of our longshoremen?

Ms. GILLIGAN. Well, again, sir, the pilot certificate was never intended as an identification medium. It was to show that the pilot was qualified for the function. Now we are trying to convert it, potentially, to an identification media, and are trying to incorporate either in that or some other single universal identification media, all the information that would be appropriate.

Mr. FARENTHOLD. It seems like more than trying. I think we—this Congress directed you to do that, didn't they?

Ms. GILLIGAN. Yes, sir, they did.

Mr. FARENTHOLD. OK. My mom used to have a saying, or a little thing she used to do to us. She would say, "Try to pick up that bottle of water." "I am trying." "We told you to pick up the bottle of water." There is a difference. I can try all day. So it was pick up the thing of water. And you can try all day long.

Let's just—it just seems to me, and like Mr. Bucshon said, the government spends too much time not talking to each other and costing too much money. So I urge you to just find a way to get her done.

Mr. MICA. Well, we will get it done, one way or the other, and with help from the members of the committee, there will be very specific direction in the FAA legislation, which should be on the President's desk before the end of May.

Any other Members—Mr. Petri has joined us. Did you—Mr. Harris? Mr. Harris?

Dr. HARRIS. Yes. Brief question, Mr. Chairman. You know, my questions were actually for the TSA folks. And, Mr. Chairman, you might enlighten me as to——

Mr. MICA. You came a little late.

Dr. HARRIS. I know. Did I miss them?

Mr. MICA. So far they have stonewalled us. They have stonewalled the Committee on Science, Space and Technology, they have stonewalled the Committee on Oversight and Government Reform. So they are——

Dr. HARRIS. Are they figuring out how to——

Mr. MICA. And we are working with the leadership and with the other committees. And, as you know, I have even threatened to subpoena. We are trying not to do that, but to enlist their support. We have had a private meeting on this subject, and they refuse to appear.

So you are coming in a little bit late in the explanation, but just to repeat for you that the two primary agencies that should be here, since TSA is also cooking up their second program for pilot identification, they are not here. So we are all frustrated by it, and we will take some steps to address it.

Dr. HARRIS. Thank you. I guess they are just figuring out how to pat down the 6-year-olds today. I mean that is probably consuming——

Mr. MICA. They have not had a good week, and——

Dr. HARRIS. It is not a good week at all. I will just be very brief, and I will just share, you know, my colleague here from—fellow physician, freshman Member—I guess I am—I share his frustration because 7 years is a long time. I thought the EPA took a long time figuring out that spilled milk on a dairy farm is not the same as an oil spill. That only took them 27 months. This is now 7 years.

And I am puzzled because I know that in the hospital—you know, I have a biometric identification to sign out narcotics and it has been there for years, and it works, and it is—you know, it is remote location, you know, I have an identification card, I have a fingerprint, it is by telecommunications, obviously transmitted some central—checks out, makes sure I am me. I mean all that technology is there.

So, you know, whatever we can do to help. I know the solutions and—are out there, and I—you know, I share the frustrations, but we ought to get it done. You know, our citizens deserve that level of security.

But thank you very much for being here. I yield back my time.

Mr. MICA. Any other Members seek recognition. Mr. Petri? No?

Well, I want to thank you all for coming out. We do not mean to beat you up too badly, particularly you, Ms. Gilligan, but there is—as you can see, there is great frustration. I know there was some differences in direction by Congress.

You have publicly stated that FAA did have problems, and was not successful in getting this out as Congress thought it should be done. We will give you some pretty specific directives, I think, in the bill that will be passed, and we will try to get this resolved quicker, and give you the tools to do that, hopefully.

But again, TSA continues to spend a countless amount of money rescreening people, and they rescreen them because they do not know who they are. And now, for pilots, they are using all kinds of identification. And we have produced, at millions of dollars, a pilot's license that is not even an acceptable form of identification. So it is very frustrating for us, as Members of Congress, to not see the agencies at least operating better, more responsibly.

We couldn't get into the TWIC program today because the program manager refused also to come before the Transportation Committee. So we really couldn't get into the problems with the nearly half-a-billion dollars that have been expended on the transportation worker identification card.

We hope that our discussions over the past couple of months with the National Institute of Standards and Technology is also helping prompt expediting the final important element, and that is a biometric standard on iris. Once we get those standards in place, we need every agency to comply and utilize the good standards that have been adopted.

We are about to recess, or adjourn the hearing. Did any other Members have any questions? Mr. Southerland?

Mr. SOUTHERLAND. I am—I just thank you, Mr. Chairman. Just a quick question.

Ms. Gilligan, I know that you have heard our frustration that TSA and Homeland Security was not here. But in your work, you know, I guess you will continue to work with these agencies. I mean tell me about your working relationship with them. I mean I am aggravated, and I certainly want the record to reflect, you know, my aggravation that we are the people's House. And when the people's House has asked, the agency has to come and give a report to the people. To me, it is a blatant disregard and a blatant disrespect to the people. It aggravates me beyond my ability, really, right now to explain.

But tell me about your working relationship with them. Since they have chosen not to come here today to address the people, what is your working relationship with them like?

Ms. GILLIGAN. Well, sir, before 9/11, the Federal Aviation Administration also had responsibility for aviation security. After that event, and the creation of the Department of Homeland Security and the Transportation Security Administration, we have had to work very closely together to assure that whatever is being put in place to enhance security does not have a negative impact on aviation safety. So we work together with TSA quite closely on many, many issues.

This issue of biometric identification for transportation workers seemed to us to be primarily their responsibility, with us assisting in whatever way we could. They have struggled. And, consequently, we have struggled with identifying what those biometric identifiers should be, the process for requiring them for the transportation worker, the creation of the infrastructure to collect the information and to have readers in locations, and to understand what is the reason for having that biometric information.

So, we continue to have those discussions. And having heard the Chairman and the Members' frustrations, I can assure you we will continue to push hard to try to come to closure on what the standards should be, and how we should create the infrastructure around the country to take advantage of that.

Mr. SOUTHERLAND. Very good. I appreciate you being here today. I look forward to furthering this issue along, and hopefully they will yield to the will of the people. And I am sure our Chairman will pursue that, as well.

So, Mr. Chairman, thank you.

Mr. MICA. Well, again, I thank our two witnesses for appearing, both a representative from the National Institute of Standards and Technology and the FAA associate administrator for aviation security.

Unfortunately, the FAA has not had a good week, neither with this hearing, unfortunately. We started off, I guess, with the Airbus 380 incident, we have had more controllers sleeping, we have a record number of mishaps. The vice chairman and I are headed right now—we are late for a meeting with the administrator, and just got word that the FAA chief administrative officer, Hank Krakowski, is resigning.

So, it is not too good a day for FAA, or too good a week. But our job is to make it better, make it work better, figure out how these things got astray, particularly during the last 4 years, and get them in order and work with the agencies and make certain that they do comply with just a common sense approach to expending limited resources, which is taxpayer dollars funding the whole show.

So, there being no further business before the Committee on Transportation and Infrastructure this morning, I thank again our witnesses, and this meeting is adjourned. Thank you.

[Whereupon, at 10:40 a.m., the committee was adjourned.]

22

Testimony of

Cita M. Furlani
Director
Information Technology Laboratory
National Institute of Standards and Technology
United States Department of Commerce

Before the

Committee on Transportation and Infrastructure
United States House of Representatives

"Biometric IDs for Pilots and Transportation Workers: Diary of Failures"

April 14, 2011

Chairman Mica, Ranking Member Rahall and Members of the Committee, I am Cita M. Furlani, Director of the Information Technology Laboratory (ITL) at the Department of Commerce's National Institute of Standards and Technology (NIST). Thank you for the opportunity to appear before you today to discuss our role in standards and testing for biometrics and identity management.

The Commerce Department's mission, as Secretary Gary Locke has reiterated time and again, is to help make American businesses more innovative at home and more competitive abroad. NIST, a non-regulatory agency within the Department, shares that overall mission, and works specifically to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

NIST accelerates the development and deployment of information and communication systems that are reliable, usable, interoperable, and secure; advances measurement science through innovations in mathematics, statistics, and computer science; and develops the measurements and standards infrastructure for emerging information technologies and applications.

NIST has more than four decades of experience improving human identification systems. NIST responds to government and market requirements for biometric standards by collaborating with other federal agencies, academia, and industry partners to:

- Support the timely development of biometric standards and associated conformity assessment.
- Develop the required conformance testing architectures and testing tools to test implementations of selected biometric standards.
- Research measurement, evaluation and standards to advance the use of image-based biometric technologies including fingerprint, face, and iris as well as multi-modal techniques.
- Develop common models and metrics for identity management, critical standards, and interoperability of electronic identities.

These efforts will improve the quality, usability, and consistency of identity management systems, protect privacy, and assure that U.S. interests are represented in the international arena.

NIST actively participates in the National Science and Technology Council Subcommittee on Biometrics and Identity Management and its Standards and Conformity Assessment Working Group. Additionally, NIST participates in the Department of Homeland Security Biometrics Coordination Group, the Department of Defense Biometrics Identity Management Agency Biometric Standards Working Group and other government groups.

NIST has developed standards to support federal agencies' information security requirements for many years, beginning in the early 1970s with enactment of the Brooks Act. Through the Federal Information Security Management Act (FISMA), Congress reaffirmed NIST's leadership role in developing standards for cybersecurity. NIST develops Federal Information Processing Standards (FIPS) when there are compelling Federal government requirements such as for security and interoperability and there are no acceptable industry standards or solutions. FISMA

provides for the development and promulgation of FIPS that are "compulsory and binding" for Federal computer systems other than national security systems. The responsibility for the development of FIPS rests with NIST, and the authority to promulgate mandatory FIPS is given to the Secretary of Commerce. Section 303 of FISMA states that NIST shall:

- have the mission of developing standards, guidelines, and associated methods and techniques for information systems;
- develop standards and guidelines, including minimum requirements, for information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency, other than national security systems; and
- develop standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems.

These activities include, for systems other than national security systems, standards and guidelines that must include, at a minimum (1) standards to be used by all agencies to categorize all their information and information systems based on the objectives of providing appropriate levels of information security, according to a range of risk levels; (2) guidelines recommending the types of information and information systems to be included in each category; and (3) minimum information security requirements for information and information systems in each category.

Under the provisions of the National Technology Transfer and Advancement Act (PL 104-113) and OMB Circular A-119, NIST is tasked with the role of encouraging and coordinating federal agency use of voluntary consensus standards and participation in the development of relevant standards, as well as promoting coordination between the public and private sectors in the development of standards and in conformity assessment activities. NIST works with other agencies to coordinate standards issues and priorities with the private sector through consensus standards organizations such as the American National Standards Institute (ANSI), the International Organization for Standardization (ISO), the Institute of Electrical and Electronic Engineers (IEEE), the Internet Engineering Task Force (IETF), and the International Telecommunication Union (ITU). NIST leads national and international consensus standards activities in cryptography, biometrics, electronic credentialing, secure network protocols, software and systems reliability, and security conformance testing – all essential to accelerate the development and deployment of information and communication systems that are reliable, usable, interoperable, and secure.

Biometric Technologies

Biometric technologies can provide a means for uniquely recognizing humans based upon one or more physical or behavioral characteristics and can be used to establish or verify personal identity of individuals previously enrolled. Examples of physical characteristics include facial images, fingerprints, and iris images. An example of learned characteristics is an individual's signature. Used with other authentication technologies, such as tokens, biometric technologies can provide higher degrees of security than other technologies employed alone. For decades, biometric technologies were used primarily in law enforcement applications, and they are still a key component of these important applications. Over the past several years, the marketplace for

biometrics solutions has widened significantly and includes public and private sector applications worldwide.

Homeland Security Presidential Directive (HSPD)-12/Federal Information Processing Standard (FIPS) 201

In response to HSPD-12 (August, 2004), NIST initiated a new program for improving the identification and authentication of Federal employees and contractors for access to Federal facilities and information systems. FIPS 201, entitled *Personal Identity Verification (PIV) of Federal Employees and Contractors,* was developed to satisfy the requirements of HSPD-12, approved by the Secretary of Commerce, and issued on February 25, 2005.

FIPS 201 incorporates three technical publications specifying several aspects of the required administrative procedures and technical specifications.

- NIST Special Publication 800-73, *Interfaces for Personal Identity Verification* specifies the interface and data elements of the PIV card;
- NIST Special Publication 800-76, *Biometric Data Specification for Personal Identity Verification* specifies the technical acquisition and formatting requirements for biometric data of the PIV system; and
- NIST Special Publication 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification* specifies the acceptable cryptographic algorithms and key sizes to be implemented and used for the PIV system.

Since the initial implementation of HSPD-12, 6.2 million PIV cards that comply with FIPS 201 have been issued to federal employees and contractors. In addition, the Department of Defense Common Access Cards (CAC) are conformant to FIPS 201.

Of particular relevance for this hearing is NIST Special Publication 800-76, *Biometric Data Specification for Personal Identity Verification,* which describes technical acquisition and formatting specifications for the biometric in the PIV system, including the PIV Card itself. This document is currently being updated (NIST Special Publication 800-76-2) to introduce the following biometric technologies for PIV use:

- Iris Image Records— the iris image for biometric authentication is a proposed addition to PIV credentials; the use of iris recognition is optional; however, iris records are required in the absence of fingerprints.
- Match on Card— privacy enhancing capability in which biometric matching is executed on the PIV credential and the enrolled biometric templates cannot be read from the card.

NIST Special Publication 800-76-2 is an important step forward in the use of biometric data for PIV. NIST, as with all of its Special Publications, is engaging the public in the development and review of the document. The document is expected to be released for public comment by April 15, 2011 with a 30-day open comment period, closing May 15, 2011. NIST will review and consider all comments received and plans to update the document by June 15, 2011. If this process results in substantive changes to the draft NIST may repeat the open comment review process to ensure all comments and issues have been adequately resolved.

Identity Credential Smart Card Interoperability: ***ISO/IEC 24727 Identification Cards-Integrated Circuit Cards Programming Interfaces***

The United States has led international efforts to address interoperability limitations and the lack of normative authentication mechanisms for improving the security and interoperability of identity management systems. In FY 2010, these efforts resulted in a new standard, *International Organization for Standardization/ International Electrotechnical Commission (ISO/IEC) 24727, Identification Cards – Integrated Circuit Cards Programming Interfaces.* This multi-part standard addresses existing ambiguities in current standards that challenge interoperability. In addition, it introduces much needed application programming interfaces and normative processes for identification, authentication, and signature services.

ISO/IEC 24727 established the architecture required to develop secure and interoperable frameworks for smart card technology based identity credentials. It enables interoperable and interchangeable smart card systems, eliminating consumer reliance on proprietary-based solutions historically provided by industry. Existing standards provide the consumer a great degree of flexibility, which can introduce challenges to achieving interoperable solutions for identity credentials, card readers, and card applications. ISO/IEC 24727 builds on these standards, fine-tuning them to improve interoperability and addressing areas that were lacking, such as a normative authentication protocols and identification, authentication, and signature services. With innovation as a central theme of our standards activities, this body of international work was developed to enable technological choices for identity management applications of the future, to include USB tokens, mobile devices, and cloud applications.

Furthering the development of formally recognized international standards through collaborative efforts with public and private sectors will support organizations in providing an interoperable and secure method for interagency use of smart card technology, in particular for identity management activities.

This standard (ISO/IEC 24727) has been publicly adopted by the European community for the European Union Citizens Card, by Germany for the German health card, and by Queensland, Australia for their next generation driver's license. We continue to work with the U.S. national standards committees to ensure compatibility with federal credentials and to address the needs of non-federal communities.

Biometric Standards to Support Interoperability of Iris Data

Draft ANSI/NIST ITL 1-2011- Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information and ISO/IEC 19794-6:2011 - Biometric data interchange formats -- Part 6: Iris image data have been updated to include Compact Iris Image Records to support iris-based verification using smart card credentials. The ANSI/NIST ITL biometric interchange format standard is primarily used for government applications. The standard is currently being revised to include a record for the use of compact iris images; interested parties will be able to review and vote on the standard this summer. ISO/IEC 19794-6:2011 is primarily a commercial industry standard which has been revised to include these types of compact iris images. These two standards are being developed in a harmonized manner that supports interoperability.

Conformance to Biometric Standards

Currently, biometric base standards for data interchange and technical interfaces do not provide specific conditions for demonstrating that products implementing the standards meet all of the technical requirements. Conformance testing to biometric standards captures the technical description of a specification and measures whether a product's implementation faithfully implements the specification. A conformance test suite is test software that is used to ascertain such conformance. NIST actively contributes to the development of technical interface standards; biometric data interchange format standards, and biometric conformance testing methodology standards.

In August 2010, we released Beta 2.0 of an Advanced Conformance Test Architecture (CTA) that supports conformance test suites designed to test implementations of biometric data interchange data formats, as well as the three components of Biometric Information Records conforming to Common Biometric Exchange Framework Format standards. NIST also released conformance test suites designed to test implementations of four American National Standard data interchange formats.

The Biometric Consortium, co-chaired by NIST and the National Security Agency (NSA), serves as a focal point for research, development, testing, evaluation, and application of biometric-based personal identification/verification technology. The Consortium's primary activity is an annual conference, which enables federal government participants to engage in exchanges with national and international participants on topics such as biometric technologies for defense, homeland security, identity management, border crossing and electronic commerce.

Conformance Tests for Transportation Worker Identification Credential (TWIC) Specifications

The Department of Homeland Security (DHS) has asked NIST to assist with their Transportation Worker Identification Credential (TWIC) specifications. The TWIC program is authorized under the provisions of the Maritime Transportation Security Act (MTSA) of 2002 (P.L. 107-295) and is a joint initiative of the Transportation Security Administration (TSA) and the U.S. Coast Guard, both under DHS. TWIC is a common identification credential for all personnel requiring unescorted access to secure areas of MTSA-regulated facilities and vessels, and all mariners must hold Coast Guard-issued credentials. TSA issued workers a tamper-resistant "Smart Card" containing the worker's biometric (fingerprint template) to allow for a positive link between the card itself and the individual. The TSA also has a requirement to establish a process to qualify products and to maintain a Qualified Technology List (QTL) for use within the TWIC program.

DHS has asked NIST to assist with the establishment of a conformity assessment framework in support of a QTL for identity and privilege credential products, to be managed by TSA. Additionally, NIST is assisting with the establishment of a testing regime for qualifying products for conformity to specified standards and TSA specifications. NIST's wealth of experience with the Cryptographic Module Validation Program (CMVP), smart card technology, and specific experience with the Personal Identity Verification (PIV) card validation program, makes NIST

uniquely qualified to assist TSA in establishing a conformity assessment program and a QTL for the TWIC Program.

In FY 2010, NIST set the framework for the conformity assessment regime for TWIC readers and for the QTL for the credential readers that successfully passed the conformity tests and satisfy all TWIC requirements.

We are currently developing, in collaboration with our partners, the conformity assessment testing suite for credential readers. NIST will continue to support DHS/TSA's efforts by assisting TSA in launching and managing the Conformity Assessment Program and the QTL.

Usability of Biometrics

The usability and ease of use of biometric systems is an overarching need and goal for deployed biometric systems within the Federal government. NIST has applied its expertise in usability and biometrics to several studies involving biometric systems in border security and airport environments. Examples of such studies are:

- NISTIR 7540 (Sept. 2008) "Assessing Face Acquisition" – the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program requested the biometrics usability team at NIST examine the current US-VISIT face image collection process to identify any usability and human factors that may improve the existing face image capture process. The report presented results of the study that examined five usability and human factors enhancements to the then current US-VISIT collection process.
- NISTIR 7504 (June 2008) "Usability Testing of Height and Angles of Ten-Print Fingerprint Capture" – this study, supported by DHS, was performed in preparation for the 10-print fingerprint capture pilot testing phase of the process through which DHS and the US-VISIT program transitioned from a two-print fingerprint capture process to a 10-print slap capture process. A concern was identified that the existing counters that housed the fingerprint scanners were too tall to support the capture process. The NIST Biometrics Usability team examined the impact on fingerprint capture performance based on angling of the fingerprint scanners at the existing counter heights. The study was designed to provide guidance on the "best" angle to position a fingerprint scanner on current counter heights in US ports of entry. As a result of this effort, all of the fingerprint scanners at US ports of entry are now angled correctly for the collection process.

NIST's usability and biometrics research was cited in the National Academies of Science (NAS) report: *Biometric Recognition: Challenges and Opportunities*, where NIST is noted as one of only two organizations addressing usability in biometric systems. The NAS Report states that "The adoption of biometric systems depends on the ease with which people can use them." and calls for "...more standardized user interfaces coupled with broader human factors testing."

Related Testing Programs

NIST Iris Exchange (IREX) Testing Program

The NIST Iris Exchange (IREX) was initiated at NIST in support of an expanded marketplace of iris-based applications based on standardized interoperable iris imagery. The work is conducted in support of the ISO/IEC 19794-6 standard and the ANSI/NIST ITL 1-2007 Type 17 standard.

- IREX I – (Nov 2007 – Jan 2010) Defined, tested, and validated accurate and interoperable Compact Iris Image Records for use on smart card credentials
- IREX III – (Announced Dec 2010) Will evaluate large-scale one-to-many iris identification algorithms.

NIST Fingerprint Minutiae Exchange (MINEX) Testing Program
NIST MINEX is an ongoing evaluation program ITL runs to test fingerprint template generators and the accuracy of fingerprint matchers using interoperable standard fingerprint minutiae templates. The General Services Administration (GSA) uses the results from this interoperability testing as criteria towards certification and inclusion on the GSA Approved Products List (APL) for FIPS 201/PIV compliant devices.

NIST's Personal Identity Verification Program (NPIVP)
NIST's NPIVP validates PIV components required by FIPS 201. The objectives of the NPIVP program are:

- to validate the compliance/conformance of two PIV components --PIV middleware and PIV card application with the specifications in NIST SP 800-73 and
- to provide the assurance that the set of PIV middleware and PIV card applications that have been validated by NPIVP are interoperable.

All of the tests under NPIVP are handled by third-party test facilities that are accredited under the Cryptographic and Security Testing (CST) Laboratory Accreditation Program (LAP) established by the National Voluntary Laboratory Accreditation Program (NVLAP) and have extended their scope of accreditation under CST LAP to include the PIV Test Methods.

Biometrics Laboratory Accreditation Program
The U.S. Department of Homeland Security has requested establishment of the Biometrics Laboratory Accreditation Program (Biometrics LAP) by NIST's National Voluntary Laboratory Accreditation Program (NVLAP) to accredit laboratories that perform conformance testing, interoperability testing, technology testing, scenario testing, and operational and usability testing for biometrics products (systems and subsystems) as defined in nationally and internationally recognized biometrics products testing standards. There are currently three laboratories that have received this accreditation.

NIST has a diverse portfolio of activities supporting our nation's biometric and identity management efforts. With NIST's extensive experience and broad array of expertise both in its laboratories and in successful collaborations with the private sector and other government agencies, NIST is actively pursuing the standards and measurement research necessary to deploy reliable, usable, interoperable, and secure identity management systems.

Thank you for the opportunity to testify today on NIST's activities in biometrics and identity management. I would be happy to answer any questions that you may have.

STATEMENT OF MARGARET GILLIGAN, ASSOCIATE ADMINISTRATOR FOR AVIATION SAFETY, FEDERAL AVIATION ADMINISTRATION, BEFORE THE HOUSE COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE ON THE INCLUSION OF BIOMETRIC IDENTIFIERS ON PILOTS LICENSES, APRIL 14, 2011.

Chairman Mica, Congressman Rahall, Members of the Committee:

Thank you for the opportunity to appear before you today on the issue of embedding biometric data on pilot certificates. I know that this issue has been of significant interest to Chairman Mica, as I have had several meetings with him on this topic. The Federal Aviation Administration (FAA) has received statutory direction on pilot certificates in the past as their potential use by other agencies was identified. I know that FAA has not acted on these directions as quickly or comprehensively as this Committee intended, but I would like to outline what FAA has done in this area and how we intend to move forward.

The FAA issues 23 different types of airman certificates. In addition to pilot certificates, these include certificates for mechanics, dispatchers, parachute riggers, and air traffic controllers. The original purpose of a pilot certificate, and the only purpose for many years, was to document that the holder met the aeronautical knowledge and experience standards established for both the certificate level and any associated ratings listed. The certificates, used for decades, worked effectively for their intended purpose.

In the late 1980s, agencies with mandates other than aviation safety began to see potential misuse of pilot certificates as law enforcement agencies engaged in activities related to the war against drugs. In 1988, the Drug Enforcement Assistance Act required FAA to

begin the process of phasing out paper certificates and replacing them with tamper resistant certificates, in an attempt to reduce pilot certificate fraud and enhance law enforcement. At that time, this was an extremely significant undertaking, affecting tens of thousands of individuals. Since October 2002, the FAA has required a pilot to carry a valid Government issued photo I.D. in addition to a pilot certificate while exercising the privileges associated with the certificate. While, as of April 2010, all pilots have plastic certificates, the effort is ongoing with respect to other certificate holders. We currently anticipate that all other certificate holders will have enhanced certificates by March 31, 2013.

After the tragic events of September 11, 2001, with aviation playing such a central role in the disaster, additional uses for pilot certificates were identified. As mentioned above, the requirement that pilots carry a government issued photo I.D. assumed that each FAA inspector who asked for pilot credentials could confirm the person about to fly was qualified and competent. In addition, if a pilot leased an aircraft, the fixed base operator could confirm both the pilot's identity and his other qualifications.

The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) imposed additional requirements on the physical license, including that it be tamper resistant and include a photograph and/or biometric identifier of the pilot. The certificates were also required to be capable of accommodating a biometric identifier, such as a digital photo or fingerprint, or any other unique identifier FAA deemed necessary.

FAA issued a Notice of Proposed Rulemaking (NPRM) in November 2010 that proposed to require that all pilots, including student pilots, possess the new certificates with a digital photo, widely acknowledged as a biometric identifier. The comment period for this rulemaking closed in February of this year. We are currently working to finalize this rulemaking within a year. Due to the broad scope and economic impact of the rule, the FAA proposed to phase-in the requirement over a five-year period. However, FAA expects that most airline pilots and flight instructors will have the new certificate within two years and that most other active pilots will have the new certificate within three years of the issuance of the final rule. FAA recognizes this timeframe is not consistent with IRTPA direction, which called for FAA to begin issuing the modified certificates in 2005. The FAA NPRM was crafted in a way to ensure compliance with IRPTA in the most cost effective and efficient manner, and we are in the process of carefully considering comments related to this NPRM to make sure that the goals of IRPTA are met in the final rule.

With respect to biometric standards, the FAA understood that other government agencies, including the National Institute of Standards and Technology (NIST) developed those standards. The FAA has been, and continues to be hopeful not to duplicate, interfere, or supersede efforts either with respect to standards or implementation. We all support the goal of enhancing aviation security and maximizing resources in order to achieve a single, universal security credential incorporating biometric data that meets a common standard. To the extent that it is practical and/or feasible, we will continue to consider how this security credential could interface with existing safety credentials. In addition,

we continue to work with TSA on a proposal to establish a universal ID for the transportation workforce.

Understanding how best to move forward to improve the use of biometric data to ensure the security of the pilot community and enhance aviation security overall will require coordination among government agencies in cooperation with airlines and industry trade associations. There is an ongoing dialogue designed to minimize duplicative efforts and to take advantage of differing areas of expertise. FAA recognizes the advantages of developing security enhancing uses for airmen biometrics and we pledge to make use of the technology as soon as it is reasonably feasible to do so. We look forward to working with this Committee as our efforts progress.

This concludes my prepared remarks. I will be happy to take questions at this time.

○