

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.