Testimony of

Charles H. Romine
Director
Information Technology Laboratory
National Institute of Standards and Technology
United States Department of Commerce

Before the

Subcommittee on Government Operations
Committee on Oversight and Government Reform
United States House of Representatives

"Standards for Biometric Technologies"

June 19, 2013

Chairman Mica, Ranking Member Connolly and Members of the Subcommittee, I am Chuck Romine, 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 as it relates to the incorporation of biometric technologies into agencies identification card programs.

The Commerce Department's mission is to help make American businesses more innovative at home and more competitive abroad. The development of technically sound measurements, testing and standards are essential for the successful deployment of technologies upon which our society depends. NIST, a non-regulatory agency within the Department 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 interoperable, secure, reliable, and usable; advances measurement science through innovations in mathematics, statistics, and computer science; and develops the measurements, testing, and standards infrastructure for emerging information technologies and applications.

NIST has nearly five 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.
- Develop the required conformance testing architectures and testing tools to test implementations of selected biometric standards.
- Research measurement, evaluation and standards to develop and advance the use of biometric technologies including fingerprint, face, iris, voice, multi-modal techniques, and emerging identity determination technologies from video.
- Develop common models and metrics for identity management, critical standards, and interoperability of electronic identities.

These efforts improve the quality, usability, interoperability and consistency of identity management systems, protect privacy, and assure that U.S. interests are represented in the international arena. In fact, NIST research has provided state of the art technology benchmarks and guidance to U.S. Industry and U.S. Government, who depend upon biometrics recognition.

To achieve this impact, NIST actively participates in the National Science and Technology Council (NSTC) Subcommittee on Biometrics and Identity Management and its Standards and Conformity Assessment and Research, Development, Test, and Evaluation Working Groups as well in several USG interagency biometric working groups.

In addition, 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 a wide variety of standards and specification developing organizations, which have vastly different models by which they develop their technical standards and specifications, but all of which are also characterized by active industry participation. NIST has about 400 NIST staff participating in approximately 120 standards and specification developing organizations. 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 interoperable, reliable, secure and usable.

BIOMETRIC TECHNOLOGY

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 face photos, fingerprints, and iris images. An example of behavioral characteristic 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 today includes public and private sector applications worldwide.

NIST'S BIOMETRIC STANDARDS ACTIVITIES

Voluntary Consensus Standards

Most Standards Developing Organizations (SDOs) are industry-led private sector organizations. Many voluntary consensus standards from those SDOs are appropriate or adaptable for the Government's purposes. According to OMB Circular A119, the use of such standards by U.S. Government Agencies, whenever practicable and appropriate, is intended to achieve the following goals:

- Eliminate the cost to the Government of developing its own standards and decrease the cost of goods procured and the burden of complying with agency regulation.
- Provide incentives and opportunities to establish standards that serve national needs.
- Encourage long-term growth for U.S. enterprises and promote efficiency and economic competition through harmonization of standards.
- Further the policy of reliance upon the private sector to supply Government needs for goods and services.

When properly conducted, standards development can increase productivity and efficiency in Government and industry, expand opportunities for international trade, conserve resources, improve health and safety, and protect the environment.

NIST Information Technology Laboratory (ITL) – An American National Standards Institute (ANSI)-accredited SDO

Under our 1984 accreditation by ANSI, the private-sector U.S. standards federation, NIST continues to develop consensus biometric data interchange standards. Starting in 1986, NIST has developed and approved a succession of data format standards for the interchange of biometric data. The current version of this standard is ANSI/NIST-ITL 1-2011, *Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information*. This standard continues to evolve to support Government applications including law enforcement, homeland security, as well as other identity management applications. This standard, used around the world, facilitates interoperable biometric data exchange across jurisdictional lines and between dissimilar systems developed by different manufacturers. In addition to the exchange of fingerprint, latent, face, and iris biometric data, the 2011 version of the standard includes new modalities (DNA and plantar) as well as a latent print extended feature set (EFS); forensic image markups for face and iris; images of all body parts, new metadata fields such as geoposition of sample collection; biometric data hashing and information assurance; and data handling logs.

NIST researchers are collaborating with biometrics and forensics experts worldwide to further expand the ANSI/NIST-ITL Standard to support forensics and Disaster Victim Identification (DVI). Currently an update is underway to include the introduction of dental data, pattern injury (e.g., bite marks) data, and forensics and investigatory voice data. The update will include new capabilities, such as x-rays and other medical imaging technologies. The additions will promote U.S. and international interoperability for forensics data pertaining to identity, and establish for the first time the exchange of dental information among various systems (such as that used by the Federal Bureau of Investigation (FBI) and INTERPOL and the ones used by medical examiners). NIST has also worked with the biometrics and forensics community to introduce within the ANSI/NIST-ITL Standard a new extended feature set to support the interoperable exchange of latent print feature data between human examiners and with automated fingerprint identification systems (AFIS).

ISO/IEC Joint Technical Committee 1, Subcommittee 37- Biometrics

From the inception of JTC 1/SC 37 in 2002, NIST has led and provided NIST experts to develop international biometric standards in this SDO. JTC 1/SC 37 developed standards have received widespread international and national market acceptance. Large international organizations, such as the International Civil Aviation Organization (ICAO) for Machine Readable Travel Documents (MRTD) and the International Labour Office (ILO) of the United Nations for the verification and identification of seafarers, specify in their requirements the use of some of the international biometric standards developed by JTC 1/SC 37.

The ICAO has moved the world's passports to a new level of travel document security, data integrity and identity management. To facilitate the goal of global interoperability, ICAO selected facial recognition as the globally interoperable biometric (listed as mandatory) for machine-assisted identity confirmation for MRTD. Additionally, ICAO selected, as options, the ability to incorporate the specifications for finger and iris. The ICAO estimate as of December 2012 was that there were 430 million ePassports existing, issued by 108 countries using the JTC 1/SC 37 standards for this application. This program serves as a model for effective collaboration and cooperation between industry through Subcommittees of ISO/IEC JTC 1 and the governments of the world through ICAO. ILO's requirements included the first edition of the finger minutiae and finger image data interchange formats developed by JTC 1/SC 37.

Representative examples of applications in different countries referring to biometric international standards include Spain (for their electronic national identity card and the Spanish e-Passports),, and India (which is deploying one of the world's largest identity assurance systems relying on standards-based biometrics technologies).

Biometric Standard for Mobile Applications

Federal agencies require that their biometric results exchange information with emerging mobile applications, making operations more effective and efficient while improving relevant information sharing associated with a biometric. NIST researchers, with support from DHS and the FBI's Biometric Center of Excellence, developed a protocol for communicating with biometric sensors over wired and wireless networks—using web technologies. The new protocol, called WS-Biometric Devices, allows desktops, laptops, tablets and smartphones to access sensors that capture biometric data such as fingerprints, iris images and face images using web services. The WS-Biometric Devices protocol enables interoperability by adding a device-independent web-services layer in the communication protocol between biometric devices and systems. This work is being developed by a private sector SDO. NIST also is working with industry through the Small Business Innovation Research Program to help bring these plug-and-play biometric devices to market.

Mobile applications typically require a rapid response over limited bandwidth communication channels. To meet performance requirements, so-called "lossy compression" must be applied, but as the name implies, data information is lost as the compression is performed, and this data loss can impact system accuracy as well as interoperability. NIST research measures and analyzes the effects of varying amounts of lossy compression and NIST is working with the biometrics community to establish biometric data transmission profiles that employ well-informed compression best practices.

Homeland Security Presidential Directive (HSPD)-12/ 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, *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. Since the initial implementation of HSPD-12, federal departments and agencies have issued PIV Cards to over 96% of federal employees and contractors. Moreover, the Administration has made strong authentication an integral part of the Cybersecurity Cross Agency Goal under the GPRA Modernization Act, shown on Performance.gov. Doing so will publicly measure how PIV cards are being used to ensure that only credentialed personnel are on Federal networks.

FIPS 201 incorporates three technical publications specifying several aspects of the required administrative procedures and technical specifications. Of particular relevance 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 has recently been updated (Draft NIST Special Publication 800-76-2) to introduce the following biometric technologies for PIV use:

- Iris Image Records— the iris image for biometric authentication has been accepted as an additional modality to PIV credentials while the collection and use of iris recognition is optional.
- On-Card Comparison (OCC) — privacy enhancing capability in which biometric matching is executed on the PIV Card and the enrolled biometric templates cannot be read from the card. OCC also provides a means of performing card activation in lieu of the PIN.
- Facial Image –The facial image provides a cost-efficient authentication mechanism for PIV Card issuance, reissuance and verification data reset processes.
- Chain-of-Trust Records -- The "chain-of-trust" is maintained by a PIV Card Issuer and allows the holder of a PIV Card to obtain a replacement for a compromised, lost, stolen, or damaged PIV Card through biometric authentication and use of the "chain-of-trust" record to personalize the new PIV Card. This capability eliminates the need for complete re-enrollment.

Draft 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 final SP 800-76-2 document will reflect the disposition of comments received from the first and second public comment periods and will be published once FIPS 201-2 is approved and published. 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.

National Security Presidential Directive/Homeland Security Presidential Directive (NSPD-59/HSPD-24), **Biometrics for Identification and Screening to Enhance National Security**

The purpose of this directive is to establish a framework to ensure that Federal executive agencies use mutually compatible methods and procedures for the collection, storage, use, analysis, and sharing of biometric and associated biographic and contextual information of individuals in a lawful and appropriate manner, while respecting their information privacy and other legal rights under U.S. law.

The recommended executive branch biometric standards are contained in the *Registry of United States Government Recommended Biometric Standards*, which is maintained by the NSTC Subcommittee on Biometrics and Identity Management. The recommended standards include ANSI/NIST-ITL 1-2011, *Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information* and other International Committee for Information Technology Standards (INCITS) and ISO/IEC biometric standards, which have been developed by INCITS M1, and JTC 1 SC 37. Critical identity management applications supported by these standards include: the FBI Electronic Biometric Transmission Specification; the DoD Electronic Biometric Transmission Specification; the DHS Automated Biometric Identification System (IDENT) Exchange Messages Specification; and the Terrorist Watchlist Person Data Exchange Standard (TWPDES).

NIST BIOMETRIC TESTING ACTIVITIES

Conformity assessment to biometric standards enables both providers and consumers to have confidence that biometric products or systems meet specified requirements. For IT, the three most important types of conformity assessment related testing are conformance, performance and interoperability testing. Conformance testing captures the technical description of a specification and measures whether an implementation (product, process, or service) faithfully implements the specification. Conformance testing does not completely ensure the interoperability or performance of conforming products, processes, or services. Therefore, interoperability and performance testing are also important for deployment of IT. Performance testing measures the performance characteristics of an implementation, such as its throughput or responsiveness, under various conditions. Interoperability testing tests one implementation with another to establish that they can work together properly. Testing, and ensuring the competence of bodies that do the testing, is as much of a market driver as the specific standard itself.

CONFORMANCE TESTING

Conformance testing to biometric standards captures the technical description of a specification and measures whether a biometric product's or system's implementation faithfully implements the specification. A Conformance Test Suite (CTS) is test software that is used to ascertain such conformance. NIST actively contributes to both biometric standards and biometric conformance testing methodology standards. These efforts also support users and product developers and the possible establishment of conformity assessment programs to validate conformance to biometric standards.

Conformance Testing for the ANSI/NIST-ITL Standard

Technical work started in 2006 with the release of a CTS designed to test implementations of a Biometric Application Programming Interface developed by the BioAPI Consortium and further work continued in the following years with the development of Conformance Test Architectures (CTAs) and CTSs designed to test implementations of national and international biometric data interchange formats (including the ANSI/NIST-ITL standards) and data structures that can contain biometric data of any modality (e.g., finger, face, and iris). In August 2010, NIST released an Advanced CTA and CTSs designed to test implementations of finger image and finger minutiae biometric data interchange formats specified in four American National Standards, and in 2011 we released a CTS designed to test implementations of the iris image data interchange format developed by ISO/IEC JTC 1/SC 37.

Work on the development of CTA and CTSs for the ANSI/NIST-ITL standards started in 2011 as well. NIST released a CTA/CTS for selected Record Types of ANSI/NIST-ITL 1-2007, and in 2012 we developed, in cooperation with other US Government agencies and industry, a Conformance Testing Methodology (CTM) for ANSI/NIST-ITL 1-2011 (published as NIST SP 500-295) and the associated CTA and CTS. In 2012 and early 2013, NIST released a number of CTSs for biometric international data interchange format standards and selected PIV profiles (including the PIV profile for iris data records specified in NIST SP800-76-2). The ANSI/NIST-ITL 1-2011 CTA/CTS is being updated to also support

data transactions encoded in XML and data specified in the expansion of the standard. CTSs designed to test implementations of international standards encoded in XML are being developed as well. NIST is also working on developing the resources to provide support for testing laboratories and users that wish to offer remote testing of biometric data interchange formats using Web Services.

Conformance Testing for Transportation Worker Identification Credential Specifications
DHS has asked NIST to assist with its Transportation Worker Identification Credential (TWIC) specifications. The TWIC program is authorized under the provisions of the Maritime Transportation Security Act of 2002 (MTSA) (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) of TWIC card readers 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 credential verification and authentication products, to be managed by TSA. Additionally, NIST is assisting with the establishment of a testing process for qualifying products for conformity to specified standards and TSA specifications. NIST's wealth of experience with the Cryptographic Module Validation Program, smart card technology, and specific experience with the 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 process for TWIC readers and for the QTL for the credential readers that successfully passed the conformity tests and satisfy all TWIC requirements. As of the end of FY 2012, three independent testing laboratories have already been accredited by NIST's National Voluntary Laboratory Accreditation Program (NVLAP) to perform TWIC reader evaluations and are now available to conduct this testing for reader vendors. Card reader products from about 20 vendors have already demonstrated the ability to meet the initial requirements.

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

PERFORMANCE AND INTEROPERABILITY TESTING

For more than a decade now, NIST has been organizing and conducting large biometric technology challenge programs and evaluations for a variety of purposes. The Multiple Biometric Grand Challenge, Face Recognition Grand Challenge and Iris Challenge Evaluation programs were conducted to challenge the face and iris recognition communities to break new ground solving research problems on the biometric frontier. The Iris Exchange (IREX) and Minutia Exchange (MINEX) programs have engaged a global community to give quantitative support for biometric data interchange standards development, to measure conformance and interoperability, foster standards adoption, and support global deployment. The Face Recognition Vendor Tests (FRVT) and the Multi-Biometric Evaluation (MBE) have been conducted to assess capabilities of face recognition prototypes for one-to-many identification and one-to-one verification. They have measured accuracy gains over the last decade that are well beyond an order of magnitude. This program has recently been expanded to test gender and age determination for emerging digital signage applications. The Speaker Recognition Evaluations (SRE) program has long challenged that community to improve speaker identification capabilities and to make implementations more robust and

versatile. The Fingerprint Technology Evaluation (FpVTE) program and Proprietary Fingerprint Template Evaluations (PFT) were developed in response to statutory mandates to established performance standards for fingerprint identification and verification.

NIST Fingerprint Minutiae Exchange (MINEX) Testing Program
NIST MINEX is an ongoing evaluation program 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 compliant devices.

NIST Face Recognition Vendor Testing (FRVT) Program
NIST FRVT provides independent evaluations of commercially available and prototype face recognition technologies. These evaluations provide the U.S. Government with information to assist in determining where and how facial recognition technology can best be deployed, and FRVT results help identify future research directions for the face recognition community. The latest FRVT (launched July 2012) evaluated large-scale one-to-many face recognition algorithms from still face photos and (for the first time) from video, along with testing automated methods for detecting pose, expression, and gender.

NIST Iris Exchange (IREX) Testing Program
The NIST IREX testing program 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 – (Jan 2010) Defined, tested, and validated accurate and interoperable Compact Iris Image Records for use on smart card credentials (e.g., PIV)
- IREX III – (April 2012) Evaluated large-scale one-to-many iris identification algorithms.

NIST Speaker and Language Recognition Evaluation (SLRE) Testing Program
NIST SLRE is an ongoing evaluation program to test and advance automated Speaker and Language Recognition capability through systematic evaluations and analysis that focuses research on the identified barriers that prevent the technology from reaching its full potential. The NIST project contributes to standardization efforts through the development of ANSI/NIST-ITL Type 11 standard, and is building a community-based scientific working group to develop best practices for Speaker Recognition as used for Forensic and Investigatory purposes.

- LRE-11 – (Dec 2011) Language Recognition Evaluation focusing research on distinguishing between confusable languages pairs and language dialects
- SRE-12 – (Dec 2012) Speaker Recognition Evaluation focusing research on the presence of environmental noise and capabilities with deeper speaker learning (vast amounts of training data).

Biometrics Laboratory Accreditation Program
DHS requested establishment of the Biometrics Laboratory Accreditation Program (Biometrics LAP) by NIST's 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. NIST Handbook 150-25, Biometrics Testing, presents technical requirements and guidance for the accreditation of laboratories under the NVLAP Biometrics Testing LAP. NIST Handbook 150-25 was developed with the participation of technical experts in the field of biometrics testing and was approved by NVLAP. The handbook is intended for information and use by accredited laboratories, assessors conducting on-site visits, laboratories seeking accreditation, laboratory accreditation systems, users of laboratory services, and others needing information on the requirements for accreditation under this program. There are presently two laboratories accredited under this program.

BIOMETRICS FOR THE NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE (NSTIC)

NIST is also working to advance biometrics through its work supporting implementation of the NSTIC. NSTIC is a White House initiative focused on the creation of an "Identity Ecosystem" where all Americans can choose from a variety of identity solutions that enable more secure, convenient and privacy-enhancing experiences everyplace they go online. Biometrics are one of many types of identity solutions that will play a role in the Identity Ecosystem.

NSTIC prescribes that identity solutions in this ecosystem adhere to four guiding principles. Identity solutions will be privacy-enhancing and voluntary, secure and resilient, interoperable, and cost-effective and easy to use.

Privacy is particularly important in NSTIC, and the Strategy calls for the Identity Ecosystem to offer improved privacy protection to individuals. Although individuals will retain the right to exchange their personal information in return for services they value, these protections will ensure that the default behavior of Identity Ecosystem providers is to:

- Limit the collection and transmission of information to the minimum necessary to fulfill the transaction's purpose and related legal requirements;
- Limit the use of the individual's data that is collected and transmitted to specified purposes;
- Limit the retention of data to the time necessary for providing and administering the services to the individual end-user for which the data was collected, except as otherwise required by law;
- Provide concise, meaningful, timely, and easy-to-understand notice to end-users on how providers collect, use, disseminate, and maintain personal information;
- Minimize data aggregation and linkages across transactions;
- Provide appropriate mechanisms to allow individuals to access, correct, and delete personal information;
- Establish accuracy standards for data used in identity assurance solutions;
- Protect, transfer at the individual's request, and securely destroy information when terminating business operations or overall participation in the Identity Ecosystem;
- Be accountable for how information is actually used and provide mechanisms for compliance, audit, and verification; and
- Provide effective redress mechanisms for, and advocacy on behalf of, individuals who believe their data may have been misused.

With its mission of catalyzing a marketplace of secure, privacy-enhancing identity solutions, the NSTIC National Program Office (NPO) has begun to explore how a number of authentication technologies including biometrics can be applied to meet the NSTIC vision and guiding principles. Last September, the NSTIC NPO awarded grants to five projects that will pilot NSTIC-aligned identity solutions that increase confidence in online transactions, prevent identity theft, and provide individuals with more control over how they share their personal information.

The five pilots were specifically selected for their potential to demonstrate innovative frameworks that can provide a foundation for the Identity Ecosystem, and tackle barriers that have, to date, impeded the Identity Ecosystem from being fully realized. The pilots span multiple sectors including health care, online media, retail, banking, higher education, and state and local government, and will test and demonstrate new solutions, models, or frameworks that do not exist in the marketplace today. Two of these pilots involve biometrics. One, led by the American Association of Motor Vehicle Administrators, will be demonstrating the use of signature as a biometric for authentication. A second, led by Daon, a private

company, will be demonstrating the use of smartphone-based voice and facial recognition biometrics for authentication. Both pilots have a two-year period of performance and in the coming months will hit "go live" milestones.

In addition, in February, 2013, the President issued Executive Order 13636 to assist private industry and promote cyber security for the Nation's critical infrastructure owners and operators. The Executive Order directs NIST to facilitate industry-led development of a framework of best practices and voluntary cybersecurity standards for core critical infrastructure.

NIST BIOMETRIC RESEARCH ACTIVITIES ADDRESSING FUTURE CHALLENGES IN BIOMETRIC TECHNOLOGIES

The "*National Biometrics Challenge 2011*" report, published by NSTC's Subcommittee on Biometrics and Identity Management, included a few key challenges to the future application of biometric technologies, including the evolution of many of the measurement, standards and testing activities described above, as well as privacy of biometrics and usability of biometrics.

Addressing Privacy of Biometrics through Technology

Biometric technologies can be used to enhance privacy and provide a convenient authentication factor for data security. Biometrics also present some new challenges in terms of protecting personally identifiable information (PII). At NIST, we are working with the international research and standards communities to advance technical methods to safeguard and control the use of biometrics. For instance, a theft of biometric information could facilitate criminal access to accounts protected with biometrics (or multi-factor authentication). The challenge to government and industry is to create solutions that allow for the use of biometrics, while mitigating security and privacy risks (e.g., identity theft or linking user accounts) through methods such as "liveness detection" and biometric template protection.

"Liveness detection" is a method that industry is developing to counter the presentation of fake biometrics (or spoofs) at a sensor, i.e., if a biometric sample is being captured from a living subject present at the point of capture. The potential for this sort of attack is mitigated in cases in which biometrics are being collected under the supervision of an officer or other personnel. Standards, best practices, and independently evaluated techniques can enable the private sector to use a wider array of multi-factor authentication technologies to protect online transactions. A future revision of FIPS 140-2 will address this topic. In addition, NIST has successfully initiated an international standards project on anti-spoofing/liveness detection within JTC 1 SC 37 (Biometrics). This is the first standards project in this field, with the goal of strengthening the security and privacy of biometrics as an authentication factor for unattended applications. NIST is leading an international "team" of co-editors and has completed the fourth official working draft.

Another issue is that of biometric template protection (also known as cancelable or revocable biometrics). Passwords are stored and validated without being revealed through modern cryptographic means, but the same techniques cannot be used for probabilistic data, such as biometrics. Biometric template protection techniques are being developed to create biometric templates (or samples) which can be used to recognize a person but do not resemble the person's original biometric. For instance, if a template is compromised through a data breach, then the affected template can be cancelled, and a new biometric template can be issued.

NIST has collaborated with the research community through a grant to advance performance metrics for evaluating these new techniques and has held a seat (as the sole U.S. representative) on the Advisory Board of an EU research project known as the TrUsted Revocable Biometric IdeNtitiEs (TURBINE) Project .

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, including:

- NISTIR 7540 (Sept. 2008) "Assessing Face Acquisition" – in response to a request from the Office of Biometric Identity Management (OBIM) (formerly the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program), the biometrics usability team at NIST examined the then-current OBIM 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 OBIM 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 OBIM 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 given the counter heights common in U.S. ports of entry. As a result of this effort, all of the fingerprint scanners at U.S. ports of entry are now angled correctly for the collection process.

NIST's usability and biometrics research was cited in the 2010 National Academies of Science (NAS) Report, *Biometric Recognition: Challenges and Opportunities*, in which NIST is identified as one of only two organizations addressing usability in biometric systems. The NAS Report notes that "[t]he 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."

IMPACTS OF NIST BIOMETRIC STANDARDS, TESTING, AND RESEARCH ACTIVITIES

NIST research has provided U.S. Government agencies (whose missions' involve biometrics collection and matching) with state-of-the-art technology benchmarks and guidance. This research has helped enhance identity systems and operations including the FBI Integrated Automated Fingerprint Identification System (IAFIS) and its new Next Generation Identification (NGI) System, the DHS Automated Biometric Identification System (IDENT)/OBIM, the DoD Automated Biometric Identification System, the Department of State Biometric Visa (BioVisa) Program, and the Intelligence Community (IC) systems.

For example, the ANSI/NIST-ITL Biometrics Interchange Standard has facilitated interoperable biometric data exchange between agencies, providing a key enabling capability for the Government to implement NSPD-59/HSPD-24. NIST biometric technology evaluations in fingerprint, face, and iris have provided the Government with timely analysis of market capabilities to guide biometric technology procurements and deployments. The FBI has co-sponsored the challenge problems and evaluations and leveraged this market analysis in its acquisition of NGI system increments. NIST research assisted DHS in its transition to ten prints within OBIM where NIST conducted usability studies for slap capture of ten prints, evaluated required slap segmentation technologies, developed supporting data exchange records, and measured the interoperability between slap and rolled fingerprints. NIST is currently working with DHS to provide standards guidance, best practices, and analysis in support of designing a biometric-enabled U.S. exit process and system.

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 interoperable, secure, reliable, and usable identity management systems. The NIST biometrics program of work continues to support the advancement of biometrics technologies while enabling the protection of individual privacy and other legal rights under U.S. law.

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