Department of Justice

STATEMENT OF

STEVEN M. MARTINEZ
EXECUTIVE ASSISTANT DIRECTOR
SCIENCE AND TECHNOLOGY BRANCH
FEDERAL BUREAU OF INVESTIGATION
U.S. DEPARTMENT OF JUSTICE

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT OPERATIONS
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
U.S. HOUSE OF REPRESENTATIVES

ENTITLED

"FEDERAL GOVERNMENT APPROACHES TO ISSUING BIOMETRIC IDS: PART II"

PRESENTED

JUNE 19, 2013

Statement for the Record
Steven M. Martinez
Executive Assistant Director
Science and Technology Branch
Federal Bureau of Investigation

Subcommittee on Government Operations
Committee on Oversight and Government Reform
U.S. House of Representatives

"Federal Government Approaches to Issuing Biometric IDs: Part II"
June 19, 2013

Good morning, Chairman Mica, Ranking Member Connolly, and Members of the Subcommittee. Thank you for the opportunity to appear before the Committee today and for your continued support of the men and women of the FBI.

I was invited today to speak to the effectiveness of using fingerprints as a secure biometric technology identifier relative to the issuance of government credentials. Please let me be clear at the outset that, while the FBI has developed deep expertise in a variety of biometric modalities, production of government identification cards, beyond our own use for physical and logical access control, is not a primary area of direct FBI responsibility. Nonetheless, the FBI was an active participant in the development of Homeland Security Presidential Directive (HSPD) 12 "Policy for a Common Identification Standard for Federal Employees and Contractors" as well as NIST Special Publication 800-73 "Interfaces for Personal Identity Verification."

The FBI issues and uses public key infrastructure (PKI) enabled individual identification cards to its employees and contractors which include a personal identification number (PIN) and at least one biometric in the form of a frontal face image. The card currently does not include a fingerprint for use in "On-Card Comparison" but it is capable of doing so. The FBI does not currently employ automated biometric matching with these identification cards. For facility access, FBI police individually compare the face image stored on the card to that of the bearer. Subsequent to FBI issuance of HSPD-12 compliant identification cards the FBI has deployed highly accurate fingerprint based identity verification technology which could in future be employed with our Personal Identity Verification (PIV) cards should the need arise. I will say a bit more about our identification verification capabilities later.

As you are likely aware, fingerprinting is a time-tested method of identifying individuals based on the friction ridge patterns and minutiae found on their fingertips. As

a general matter, no two persons have been found to possess the exact same sets of fingerprints and those fingerprints are persistent throughout one's lifetime. Even identical twins have different fingerprints. Fingerprints can be recorded on a standard fingerprint card or recorded electronically. By comparing known fingerprints to collected fingerprints, officials can establish the identity of a person in a quick manner.

History

The use of fingerprint identification in the United States dates back to 1902. The New York Civil Service Commission established the practice of fingerprinting applicants to prevent them from having better qualified persons take their tests for them. The New York state prison system began to use fingerprints for the identification of criminals in 1903. In 1904 the fingerprint system accelerated when the United States Penitentiary at Leavenworth, Kansas, and the St. Louis, Missouri, Police Department both established fingerprint bureaus. During the first quarter of the 20th century, more and more local police identification bureaus established fingerprint systems. The growing need and demand by police officials for a national repository and clearinghouse for fingerprint records led to an Act of Congress on July 1, 1921, establishing the Identification Division of the FBI. In 1933, the United States Civil Service Commission, known today as the Office of Personal Management, submitted 140,000 government employees' fingerprints and applications to the FBI precipitating the creation of the Civil Identification Section. In 1992, the FBI Identification Division was restructured as the Criminal Justice Information Services Division, or CJIS, now located in Clarksburg, West Virginia.

Use of Fingerprints

The FBI uses fingerprints in two primary ways: background checks and criminal investigations.

A criminal history record, or a "rap sheet", is a catalog of information taken from fingerprint submissions in connection with arrests and in some instances, federal employment, naturalization, or military service. When fingerprints are related to an arrest, the Criminal History Summary includes name of the agency that submitted the fingerprints to the FBI, the date of the arrest, the arrest charge, and the disposition of the arrest. All arrest data included in a Criminal History Summary is obtained from fingerprint submissions, disposition reports, and other information submitted by agencies having criminal justice responsibilities.

Fingerprints recovered from evidence found at crimes scenes are processed through our Latent Print Operations Unit (LPOU) located at the FBI Laboratory in

Quantico, VA. These prints, typically referred to as latent prints, are examined and used to assist in criminal investigations. The LPOU also uses fingerprints to assist in the identification of victims from natural disasters and mass fatalities. Such events include: Hurricane Katrina, the Thailand Tsunami, the Oklahoma City bombing, TWA Flight 800, the Space Shuttle Challenger explosion, the attack on the USS *Cole*, and the 9/11 terrorist attacks.

Modern Fingerprint Matching as a Criminal Justice Information Service

Originally, fingerprint identification and matching were performed manually by trained fingerprint examiners in a laboratory. Today, the practice has evolved through the use of computers into a highly automated and reliable process. Currently, more than 18,000 local, state, tribal, federal, and international partners electronically submit requests to the FBI's Integrated Automated Fingerprint Identification System (IAFIS) housed and maintained by the CJIS Division. However, advances in technology, customer requirements, and the growing demand for IAFIS services, compelled the FBI to create the Next Generation Identification or NGI Program in order to bring identification services to the next level. The NGI Program is advancing the FBI's biometric identification and investigation services by providing an incremental replacement of current IAFIS technical capabilities, while introducing new biometric functionality. With NGI, the FBI is dramatically improving all of the major features of the current IAFIS, including system flexibility, storage capacity, accuracy and timeliness of responses, and interoperability with other systems, such as the biometric matching systems of the Department of Homeland Security (DHS) and the Department of Defense.

NGI is being developed and deployed incrementally. The initial increment included the launch of the NGI Advanced Fingerprint Identification Technology (AFIT) on February 25, 2011, which replaced the Automated Fingerprint Identification System (AFIS) segment of the IAFIS and provided the following: faster algorithm processing; increased "lights out" processing (without staff intervention) for sequence check and image comparison; improved search accuracy; new validation algorithm for image quality and sequence checks; and improved flat print searching. Enhancements to the system have decreased the transaction rejection rate due to a better ability to process poor image quality probe and exemplar submissions. The NGI accuracy is currently measured at 99.6 percent. Prior to IAFIS the FBI had rare false matches reported to contributors, approximately 1 per 50,000,000. There have been no known false matches since IAFIS initial operability with nearly ½ billion fingerprint checks conducted. Further, these technology advancements have also provided the ability for FBI to respond to criminal submissions with an average of only 8 minutes, 52 seconds.

NGI's second increment, the Repository for Individuals of Special Concern (RISC) was completed in August 2011, and provides mobile access for law enforcement officers nationwide through hand-held devices that submit fingerprints of high interest individuals against a repository of wanted criminals, terrorists, and sex offenders. Rapid responses are received in the field in a red, yellow, or green format. Eleven states are currently participating in the RISC and nearly 800,000 RISC transactions have been processed to date.

Capabilities in relation to latent and palm prints, rapid DHS response, and full infrastructure were rolled out as part of the third increment, completed in May of this year (2013). All contributors immediately benefited from 3 times increased accuracy, and now have access to a National Palm Print Repository, which continues to grow. Some U.S. Customs and Border Protection, Ports of Entry Primary, now have access to a 10-second search of the system's full Criminal Master File of biometric-based criminal history information. The expanded cascaded searches of the Unsolved Latent File have already produced potential matches.

The fourth increment, expected to be delivered in June 2014, will include replacing the legacy system functionality and adding new services of Rap Back and the Interstate Photo System. The Rap Back Service will provide an on-going status notification of any change in criminal history (e.g., an arrest or a conviction) reported to the FBI after an individual's initial criminal history check. This service can be used both for noncriminal justice applicants, employees, volunteers, licensees, etc., and for individuals under criminal investigation or under the supervision of criminal justice agencies. The Interstate Photo System Facial Recognition Pilot is a collaboration among the FBI and state law enforcement agencies to assess NGI face search capabilities on real data. Authorized law enforcement partners can search more than 15.2 million criminal face images, or "mug-shots."

The final increments of NGI will include an effort to provide identification based on iris images, scheduled for pilot deployment in 2013, and a focus on technology refreshment.

Since automation through IAFIS, the FBI has processed more than 456 million fingerprint submissions. The current reject rate on these submission is 3.77% (Note: average error rate over the last 13 months), with most of these (3/4) due to poor image quality.

Other Biometrics

The FBI has long been a leader in the development and use of biometrics. While fingerprints may be considered the most common and widely used biometric modality, other biometrics await just beyond the horizon and the FBI is actively researching their accuracy, reliability and potential suitability in the lawful and Constitutional performance of our mission. The FBI is, for example, a recognized leader in forensic deoxyribonucleic acid (DNA) identification and has been a leader in the development of Rapid DNA identification equipment to allow use of DNA as a biometric element of identification during the criminal booking process. As just mentioned, face identification services, matching police photo submissions to mug shots collected during the criminal booking process is a planned capability of the Next Generation Identification (NGI) System which is currently under development. Iris has proven to be an effective modality for prisoner custodial management and transfer applications. NGI is developing a pilot project that will assess the cost effectiveness of iris matching as an NGI service. The FBI also conducts forensic speaker identification analyses. To further explore and advance the use of new and enhanced biometric identity management technologies and capabilities, the FBI created the Biometric Center of Excellence (BCOE), headquartered at the CJIS Division in Clarksburg, WV.

I'd like to address briefly some of the other biometric modalities, beyond fingerprints, that the FBI is evaluating.

The computer-based facial recognition industry has made useful advancements in the past decade, facilitated in no small measure through the standards of the National Institute of Standards and Technology (NIST), DHS, and the FBI. However, the need for higher accuracy remains. Through the determination and commitment of industry, government evaluations, and organized standards, growth and progress continue raising the bar for this technology.

Palm print identification, just like fingerprint identification, is based on the aggregate of information presented in a friction ridge impression. This science is still relatively new and there have been large advances with continued studies and research.

Iris recognition is the process of recognizing a person by analyzing the random pattern of the iris. The automated method of iris recognition is relatively young, existing in patent since 1994, therefore a need for continued research and testing remains. DHS and the Intelligence Technology Innovation Center co-sponsored a test of iris recognition accuracy, usability, and interoperability referred to as the Independent Testing of Iris Recognition Technology.

Speaker recognition relies on voice recognition (not to be confused with "speech recognition,") which recognizes words as they are articulated and does not yield a biometric signature). The speaker recognition process relies on both the physical structure of an individual's voice and the individual's behavioral characteristics. Both National Security Agency and NIST are committed to further research and with their collaboration, speaker recognition will continue to evolve.

DNA is another popular biometric modality. A DNA profile comes from biological samples such as blood, saliva, hair, semen, or tissue. The benefit of using DNA as a biometric identifier is the level of accuracy offered. For example, with 13 different bands used today, the chance of two individuals sharing the same DNA profile is rarer than one in a 100 billion.

Finally, the FBI's BCOE will be looking at the potential of emerging biometric technology to allow federal and local law enforcement partners to increase their identity management capabilities. The BCOE will also work on developing and enhancing other potential new biometric technologies including footprint and hand geometry, gait recognition.

Conclusion

Chairman Mica and Ranking Member Connolly, I thank you for this opportunity to discuss the FBI's fingerprint and biometric programs.

I look forward to any questions that you may have.