Statement for the Record
of
Kathleen Kraninger
Deputy Assistant Secretary for Policy, Screening Coordination
Department of Homeland Security
and
Robert A. Mocny
Director
US-VISIT Program
National Protection and Programs Directorate
Department of Homeland Security

Before the
United States House of Representatives
Appropriations Committee, Subcommittee on Homeland Security
Washington, DC

March 19, 2009

Chairman Price, Ranking Member Rogers, and other distinguished Members, we are pleased to appear before you today to discuss how the use of biometrics and identity management programs enhances our Nation's security. The Department of Homeland Security (DHS) continues to refine our capabilities to identify accurately and more efficiently process individuals at the border, in airports, and across our screening programs. The Screening Coordination Office (SCO) within the DHS Office of Policy was established to integrate, where appropriate, the wide range of DHS screening and credentialing activities to enhance our missions of keeping dangerous people and things out of the U.S. and securing critical infrastructure. US-VISIT provides the Department's biometrics identification and analysis services to agencies throughout the immigration and border management, law enforcement and intelligence communities. US-VISIT supports the Department's mission by providing biometric identification services to Federal, State and local government decision-makers to help them accurately identify people and assess risk.

Access to our nation is critical for a terrorist to plan and carry out attacks on our homeland. As the 9/11 Commission's Final Report states, "Terrorists must travel clandestinely to meet, train, plan, case targets, and gain access to attack. To them, international travel presents great danger because they must surface to pass through regulated channels to present themselves to border security officials, or attempt to circumvent inspection points." As the Department continues to implement and integrate key screening programs, the establishment of an integrated immigration and border screening system represents a significant achievement that has improved national security.

The Value of Biometrics

The Department began to collect digital fingerprints and photographs from international visitors applying for visas or arriving at U.S. ports of entry (POE) in 2004 to help immigration officials make visa-issuance and admission decisions. With biographic screening capabilities already

well established, biometrics became the next logical step in the evolution of identity management. Unlike names and dates of birth, biometrics are unique and extremely difficult to forge. They provide a reliable, convenient, and accurate way to establish and verify visitors' identities. Moreover, biometrics are a scalable technology and can be upgraded to stay one step ahead of terrorists and criminals. Biometrics help us meet the challenge of making travel difficult for those who want to do us harm, while making it convenient and efficient for legitimate visitors.

Through its use of biometrics, the Department's US-VISIT program collects, stores, and shares digital fingerscans and digital photographs for subsequent verification. This biometric information is paired with biographic information pertaining to an individual and used to establish and verify that individual's identity.

We want to reinforce the critical progress we have made by discussing key capabilities that biometrics provide: greater security, increased efficiency, and a new level of identity assurance.

The Department's implementation of biometrics capabilities has laid the foundation for the rapid expansion of biometric identification to other agencies. Today, this biometric coordination across the Government is making our screening more collaborative, more streamlined, and more effective than ever before.

Five years ago, our immigration and border management system had disparate information systems that lacked coordination. Today, the Department is unifying these systems to promote a centralized source for biometric-based information on criminals, immigration violators, and known or suspected terrorists.

Five years ago, U.S. Immigration and Customs Enforcement (ICE) lacked timely and accurate information about visitors who overstay their visas. Today, US-VISIT provides more than 250 credible leads weekly to ICE, enabling that organization to better enforce our immigration laws. Through ICE's Secure Communities Program, we are also helping to identify immigration violators arrested by State and local law enforcement.

Five years ago, the United States was alone in applying biometrics to the immigration and border management communities. Today, the United Kingdom and Japan already have robust programs using biometrics. The European Union, Canada, Mexico, Australia, Argentina, Peru and many other countries are in various stages of applying biometrics to immigration control.

Five years ago, we were relying on visual inspection of travel documents to try to identify those that were fraudulent. Today, because of increased information sharing within DHS and with the Department of State (DOS), along with the use of biometrics and machine-readable travel documents, we are able to more quickly identify fraudulent documents. As an example, DHS and DOS partnered in developing the e-passport, which set a new international standard for the security features of a travel document, and the passport card, providing U.S. citizens a secure, limited-use travel document in a more convenient format.

As you know, DHS is preparing for the June 1, 2009, implementation of the Western Hemisphere Travel Initiative (WHTI), which will require U.S. and Canadian citizens to present standardized, secure documentation denoting identity and citizenship for entry at the U.S. land and sea ports of entry. WHTI addresses the vulnerabilities inherent when travelers can present a wide range of documents that are highly susceptible to fraud and cannot be verified. WHTI-

compliant documents available to U.S. citizens (the passport book, passport card, Trusted Traveler Program cards, and Enhanceds Driver's Licenses) are issued in a secure manner and include a biometric (digital photograph) on the face of the card. The WHTI solution is transforming the border by moving away from a vehicle-centric system to a person-centric one.

Radio-frequency identification technology embedded in most WHTI-compliant travel documents, with the appropriate privacy protections and infrastructure, allow DHS the ability to verify an individual's identity and perform real-time queries against lookout databases even before the traveler pulls up to the inspection booth. The trained DHS officer can compare the digital photograph and biographic information on the document to the traveler in front of them, as well as to the photograph and information on the DHS border officer's screen that is provided by the document's issuer—all of which assist the officer in making better decisions about an individual's admissibility to our country.

While implementing the screening programs across the Department, DHS has maintained focus on the four guiding principles first established for US-VISIT, which are to:

- Enhance the security of our citizens and visitors;
- Facilitate legitimate travel and trade;
- Ensure the integrity of our immigration system; and
- Protect the privacy of our visitors.

Screening and Credentialing Programs

DHS continues to identify opportunities to harmonize and enhance screening processes for both security and efficiency reasons across DHS programs. In doing so, we must rationalize and prioritize investments in screening technologies and systems while recognizing that each program faces individual challenges, operates in different environments, and adheres to its respective legal authorities.

In July 2008, DHS finalized the DHS Credentialing Framework Initiative (CFI) to guide the selection and coordination of credentialing activities and investments throughout DHS. In developing the CFI, the SCO led a DHS-wide effort to analyze and compare key programs across the credentialing lifecycle of registration and enrollment, eligibility vetting and risk assessment, issuance, and expiration and revocation; identify the relationships between the credentialing processes and business capabilities and the Information Technology services related to screening and credentialing across the DHS enterprise; and outline the projects needed to actualize a robust, cohesive environment across DHS programs.

While one size does not fit all, every program does not have to reinvent the wheel. The CFI aims to provide a consistent, security risk-based framework across all DHS credentials, improve credentialing processes to eliminate redundant activities, utilize existing information more effectively and improve the experience for individuals applying for DHS credentials. The guidance directs the following:

- Design credentials to support multiple licenses, privileges, or status, based on the risks associated with the environments in which they will be used.
- Vetting, associated with like uses and like risks, should be the same.
- Immigration status determinations by DHS components should be verified electronically.
- Eligibility for a license, privilege, or status should be verified using technology.

- Design enrollment platforms and data collection investments so that they can be reused by other DHS programs – establishing a preference for "enroll once, use many" environment, where appropriate.
- Ensure opportunities for redress – individuals should be able to correct information held about them.

Integrating a Streamlined Transportation Screening Platform

The Transportation Security Administration's (TSA) Transportation Threat Assessment and Credentialing (TTAC) entity is in the initial stages of an enterprise modernization that is being designed to meet the mission of TSA in line with the CFI requirements. The TTAC Enterprise Modernization Program supports TSA's mission by significantly improving the vetting management and adjudication platform currently used for conducting security threat assessments on various transportation populations through the use of software applications and a common information technology infrastructure. The current TTAC vetting and credentialing enterprise architecture was created to support 2.5 million individuals per year. Today, the populations supported by TTAC have almost tripled.

It is anticipated that after five years, existing stove-piped business processes and information systems will either be reengineered or replaced by a new integrated business enterprise architecture that will: consolidate multiple enrollment methods, implement identity management services across programs, standardize the approach for customer relationship management, standardize the physical and virtual credentialing processes, standardize threat assessment processes, and consolidate operations, integrating program-specific IT systems and business processes into a common secure enterprise vetting and credentialing architecture. The TTAC Enterprise Modernization program presents an opportunity to eliminate redundant business practices, processes, and subsequent IT investments to achieve significant economies of scale benefits associated with a unifying business integration effort.

In line with the CFI, the TTAC Enterprise Modernization program provides for a unified, modular, and maintainable architecture that will reduce the cost, risk, and time associated with implementing new capabilities, on-boarding new populations, improving the robust nature of the architecture, and on-going operations and maintenance. The Department expects that TTAC modernization will support not only TSA needs but also other special population vetting programs that may support the security of critical infrastructure sectors. Further, TTAC modernization is being coordinated with the Department's other ongoing information technology modernization efforts.

Biometric Screening and Identification

In another effort to streamline DHS processes, DHS has designated US-VISIT's Automated Biometric Identification System (IDENT) as the biometric storage and matching service for the Department, providing biometric identification and analysis services to agencies throughout the immigration and border management, law enforcement, and intelligence communities. US-VISIT supplies the technology for collecting and storing biometric data, provides analysis of the data to decision-makers, and ensures the integrity of the data.

IDENT plays an important role in the biometric screening and identity verification of non-U.S. citizens for ICE, CBP, U.S. Citizenship and Immigration Services (USCIS), and U.S. Coast

Guard. US-VISIT also supports the Department of State's (DOS) BioVisa Program and shares information with the Federal Bureau of Investigation (FBI).

Here is how it works:

- With each encounter, US-VISIT checks a person's biometrics against a watchlist of more than 5.2 million known or suspected terrorists, criminals, and immigration violators identified by U.S. authorities and Interpol.
- When an identification document is presented, a person's biometrics are also checked against those DHS has on file as associated with the document to ensure that the document belongs to the person presenting it and not to someone else.
- US-VISIT provides the results of these checks to decision-makers when and where they need them.

Biometric Services for DHS and Other Agencies

To give you an idea of the breadth of our services, every day US-VISIT provides access to biometric data for 30,000 authorized Federal, State, and local government agency users to help them identify, mitigate, and eliminate security risks. Let us give you a few examples.

- USCIS uses biometrics to screen applicants for immigration benefits.
- Border Patrol and U.S. Coast Guard use biometrics as part of their efforts to apprehend illegal migrants.
- Department of Defense (DOD) and the intelligence community provide biometrics, including latent fingerprints, they collect from locations where terrorists have been, such as safe houses or training camps to DHS in order to determine whether we've previously encountered individuals they suspect to be terrorists and terror suspects.
- And finally, State, local and other federal agencies submit biometrics to DHS to support their investigations. Our Biometric Support Center (BSC) verifies almost 50,000 fingerprints each week—helping to solve crimes, identify John or Jane Does, and support terrorist investigations.

Additionally, the US-VISIT Program Office is working with a number of other DHS components, such as the TSA, on future and planned credentialing and identity management programs.

10-Fingerprint Transition

DHS's transition from collecting 2 digital fingerprints to collecting 10 digital fingerprints at ports of entry from visitors to the United States is nearly complete. DHS deployed new 10-fingerprint scanners at U.S. POEs in 2008, providing the capability to capture 10 fingerprints from 97 percent of in-scope travelers. The transition to 10-fingerprint collection increases DHS's ability to keep dangerous people out of the United States, while making legitimate travel more efficient. Today, the new fingerprint scanning devices are in place at all major POEs, so international visitors can expect to use the upgraded technology when they enter the United States.

The use of 10 fingerprints for biometric verification offers many enhancements. In 2007, DOS began collecting 10 fingerprints from visa applicants at all of our embassies and consulates to

enhance the ability to establish and verify applicants' identities. 10-fingerprint readers improve the accuracy of identification; improve interoperability with the FBI and DOS, local, and tribal governments; and will mean fewer travelers will be referred to CBP secondary inspection. DHS will now also be able to conduct full searches against the FBI Unsolved Latent File, which, for example, allows DHS to match against prints lifted from crime scenes and those collected in Afghanistan and Iraq.

Interoperability with the Departments of Justice and State

DHS's 10-fingerprint collection standard makes our system more compatible with the FBI's biometric system, the Integrated Automated Fingerprint Identification System (IAFIS). We have been working with the FBI for the last several years to make our two databases fully interoperable to more seamlessly match biometric information so we can better identify people who pose a threat to our country.

DHS, the Department of Justice (DOJ), and DOS signed a memorandum of understanding on interoperability on August 1, 2008. The first-phase capabilities for the initial operational capability were deployed in October 2008.

This integrated system will allow authorized users access to all relevant information in a timely manner so they can make the right decisions about the individuals they encounter. IDENT/IAFIS interoperability increases the ability of DHS and DOS to screen individuals; and it benefits the FBI and other law enforcement organizations by providing them with increased access to immigration information about high-risk individuals to whom DOS has refused visas and those whom DHS has expeditiously removed.

Secure Communities

The Department's Secure Communities initiative will change immigration enforcement by using technology to automate sharing with law enforcement agencies and by applying risk-based methodologies to focus resources on assisting all local communities to remove high-risk criminal aliens.

In 2008, DHS and DOJ began an information-sharing program with local law enforcement counties in North Carolina by providing them access to immigration violation information on their criminal arrests. This capability is part of DHS and DOJ efforts to distribute integration technology that will link local law enforcement agencies to both FBI and DHS biometric databases.

US-VISIT and the FBI Criminal Justice Information Services Division continue to work with ICE in preparation for further deployment of Secure Communities.

Developing Interoperability with the Department of Defense

DHS and DOD have begun identifying ways the two departments can exchange information in a more systematic manner to further each other's missions consistent with legal authorities and privacy. Central to this effort is an automated exchange of biometric data on individuals' DOD encounters overseas. Such information would greatly enhance the ability of DOS and DHS to effectively screen who is admitted into the United States. DHS information is useful to DOD for credentialing and access control vetting, among other uses. As with interoperability with DOJ

and DOS, some of the most complex issues concerning data sharing are not technical, but rather those dealing with policy and business processes. DHS and DOD are working diligently to explore potential opportunities and to identify technical and process solutions.

Air/Sea Biometric Exit

DHS has performed significant planning and testing over the past three years examining possible solutions for integrating US-VISIT biometric exit requirements into the international air departure process. The options of deployment at airline ticket counters, TSA checkpoints, airline boarding gates, and in airport terminals are being considered. For more than two years, US-VISIT ran biometric exit pilots at 14 air and sea locations. These pilots evaluated the use of both automated kiosks and mobile devices in port terminals. The pilots ended in May 2007 and demonstrated that the technology works, but also that compliance by travelers was low.

On April 24, 2008, DHS published a notice of proposed rulemaking (NPRM) on the collection of biometrics from aliens departing from air and sea ports. The NPRM proposed that commercial air carriers and vessel carriers collect and transmit international visitors' biometric information to DHS within 24 hours of their departure from the United States. Development and publication of a final rule is pending the completion of pilots as required by the Consolidated Security, Disaster Assistance, and Continuing Appropriations Act, 2009 (Pub. Law 110-329). The 2009 Appropriations Act restricts US-VISIT from spending any money to create an air exit solution, until the pilots are completed and a report on the pilot test is submitted to the Committees on Appropriations of the Senate and the House of Representatives and reviewed by GAO. DHS is assessing methods for conducting air exit pilots consistent with the FY 2009 appropriation. The results of the pilot evaluation, combined with the review of public comments submitted in response to the NPRM, will inform the decision on the option to be selected for publication in the final rule.

When a long-term exit solution is deployed, it will also be deployed to commercial seaports to provide an integrated biometric exit capture for vessel carriers passengers. However, the scope for biometric exit at sea will be considerably smaller than for air.

International Cooperation and Collaboration

When DHS began the US-VISIT program to collect biometrics as part of port of entry screening, the world watched skeptically to see if the benefits of biometrics would work on a large scale. Although a handful of nations were testing biometrics, DHS was the first to launch a comprehensive biometric-based identity management system for immigration and border management. Five years later, more and more countries are approaching us to discuss our lessons learned as they develop their own similar systems. We want other countries to benefit from our experience, and in turn, we can learn from them.

Some countries have already begun operations or are nearing deployment. For example:

- In November 2007, Japan implemented a two-fingerprint biometric entry system that is similar to US-VISIT's initial implementation.
- The United Kingdom is collecting 10 fingerprints from visa applicants and is testing fingerprint collection at ports of entry.

- The European Union is building a 10-fingerprint visa-issuance program based on the very successful Eurodac.
- We are working closely with Australia, which has been a pioneer in facial recognition, as it advances its identity management program.
- The United Arab Emirates has been using iris scans as part of its immigration and border control processes for some time now.

Other countries are actively pursuing biometrics:

- In August 2008, Peru announced it is working to implement biometric technology in its migration control systems to guarantee the authenticity of personal identification documents and to speed visitor control.
- Mexico is planning to modify its currently successful biographic-based system to incorporate biometrics, which is similar to what we did in 2004.
- Canada recently approved the budget for a 10-fingerprint visa-issuance program.

As the use of biometrics increases worldwide, the importance of international standards and best practices cannot be overstated. Consistent international standards for biometrics are essential to developing compatible systems, and compatible systems are essential to crippling international criminal enterprises as well as terrorists' ability to travel. Appropriate data sharing can only be accomplished with consistent standards.

The Future of Biometric Screening

Biometrics offer real opportunities to dramatically increase the efficiency of identifying people. The Department is researching emerging technologies to expand our screening and identification capabilities. We recognize that future identity management systems will require increased assurance, efficiency, ease of use, and flexibility.

As DHS implements biometric exit procedures, both at airports and land border POEs, we are looking for more efficient, less invasive technologies to verify visitors' departures. Particularly at the land border, we are looking for technologies that might meet our needs better than requiring visitors to have their fingerprints scanned while driving at speed through a POE.

In some cases, the key to expanding biometric screening is to bring the technology to remote locations where decision-makers need it.

- For example, Coast Guard is using mobile biometric collection and analysis capabilities on the high seas off the coasts of Puerto Rico and Florida. This project has helped the Coast Guard identify and refer for prosecution and/or administrative immigration proceedings hundreds of repeat illegal migrants who are ineligible to enter the United States, including some wanted for human smuggling and murder.
- In addition, CBP's Air and Marine Operations is examining opportunities to use mobile biometrics to its areas of operation.

Success Stories

Our biometric entry procedures have made a tremendous difference in efforts to improve the integrity of our immigration and border management system. Some of our many success stories include stopping more than 2,400 criminals or immigration violators at the POEs based on

biometrics alone, and identifying thousands who are ineligible to receive visas to travel to the United States. There is no doubt that we have deterred countless more.

DHS's use of biometrics is helping eliminate the ability to use fraudulent or altered travel documents. Now when travelers arrive in the United States, we are able to quickly verify their identity and identify those who are known to have committed immigration violations. Here is an example:

- On March 16, 2008, a subject arrived at the John F. Kennedy International Airport in New York and applied for admission with a valid Turkish passport and an unexpired B1/B2 visa. The subject was referred to secondary inspection as a match to the IDENT biometric watchlist for a previous voluntary departure.
- During secondary inspection, queries revealed that on November 10, 2003, the subject had been apprehended taking pictures of the Ft. Leonard Wood Missouri Military Base. While in custody, it was discovered then that he had overstayed his period of admission in the United States.
- This subject had been admitted into the United States on June 9, 1997, and was granted voluntary departure by an immigration judge on May 13, 2005, to remove himself by September 13, 2005.
- On March 16, 2008, the subject attempted to enter the United States using the identity of his twin brother through his brother's travel documents. The subject was denied access. The subject is inadmissible to the United States for willful misrepresentation and not being in possession of valid travel documents.

Biometrics are helping enforce our borders away from ports of entry, too.

- In December 2007, the U.S. Coast Guard interdicted 10 migrants attempting to illegally enter Puerto Rico by sea. When the migrants' biometrics were checked against IDENT, it was revealed that two of the migrants had illegally entered the United States before, had been subsequently removed from the United States, and were suspected of being part of a human trafficking organization. The two suspected traffickers were brought ashore for referral for prosecution along with two witnesses who would testify against them. Since the Coast Guard began using mobile biometric services to identify illegal migrants at sea, prosecutions of repeat offenders have increased dramatically and illegal migration has dropped by 60 percent in the area where the technology is being used.

US-VISIT Privacy

DHS is committed to adhering to the strictest privacy standards. DHS only collects information needed to achieve the program objectives and mission and only uses this information in a manner consistent with the purpose for which it was collected. DHS also conducts periodic audits of its systems to ensure appropriate use within the limitations of the Privacy Act.

Ultimately, the success of the US-VISIT program will be measured by not only our ability to identify those who may present a threat, but also our ability to protect against identity theft and fraud. We are acutely aware that our success depends on how well we are able to protect the privacy of those whose biometrics we hold. A breach of this most personal data would undermine the public's trust. We have a dedicated privacy officer responsible for ensuring compliance with privacy laws and procedures and for creating a culture of privacy protection

within the US-VISIT Program. Furthermore, we are transparent. From the beginning, we made clear that the information gathered by DHS or State will be used only for the purposes for which it was collected, consistent with those uses authorized or mandated by law. Our policy extends to non-U.S. citizens most of the same privacy protections we give by law to U.S. citizens. We regularly publish privacy impact assessments and system of records notices to provide people with a clear view of the information we collect, how we store it, and our policies and practices to ensure it is not abused.

Conclusion

To ensure we can shut down terrorist networks before they ever get to the United States, we must also take the lead in driving international biometric standards. By developing compatible systems, we will be able to securely share terrorist information internationally to bolster our defenses. Just as we are improving the way we collaborate within the U.S. Government to identify and weed out terrorists and other dangerous people, we have the same obligation to work with our partners abroad to prevent terrorists from making any move undetected. Biometrics provide a new way to bring terrorists' true identities to light, stripping them of their greatest advantage—remaining unknown.

Biometrics have increased our Nation's security and the security of nations around the world to a level that simply did not exist before. Biometrics are affording us greater efficiencies, making travel more convenient, predictable, and secure for legitimate travelers. Biometrics are enabling people to have greater confidence that their identities are protected, and in turn decision-makers are more certain that the people they encounter are who they say they are.

So what is next? We need to aggressively pursue innovation. Those who want to do us harm continue to contemplate ways to exploit our weaknesses, so we cannot afford to slow down. We too must contemplate ways to create even more efficient and affordable identification technologies. We have to continue to explore mobile biometrics and biometrics captured at speed, and we must do so safely.

We must also continue to advocate abroad. We recognize that with the power of biometrics and a foundation of international cooperation, we can transform and enhance the way the people travel the world and the way we protect our nations from those who would do us harm.

Chairman Price, Ranking Member Rogers, and other distinguished Members, we have outlined our current efforts that, with your assistance, will help DHS continue to protect America. The Department's use of biometrics plays a critical role in supporting many programs and initiatives within DHS and other Federal agencies.

Thank you for again for this opportunity to testify. We will be happy to answer any of your questions.