UNITED STATES DEPARTMENT OF HOMELAND SECURITY

STATEMENT OF KATHLEEN KRANINGER
DIRECTOR, SCREENING COORDINATION OFFICE

Before the

UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON HOMELAND SECURITY -
SUBCOMMITTEE ON TRANSPORTATION SECURITY
AND INFRASTRUCTURE PROTECTION

October 18, 2007

Good afternoon Chairman Towns, Ranking Member Bilbray, and distinguished members of the Subcommittee. Thank you for this opportunity to discuss the ongoing efforts of the Department of Homeland Security (DHS) to secure identification documents, thereby improving the way we screen and process people. Identity documents provide one means of demonstrating, with varying levels of assurance, that an individual is who they say they are. As such, they form the basis of the screening process. The ability to quickly and accurately confirm a person's identity and check it against watch lists to identify potential hostile intent is crucial to the Department's mission.

The Screening Coordination Office, which I direct, was established by Secretary Chertoff last summer to integrate, where appropriate, DHS screening and credentialing activities to enhance our missions of keeping dangerous people and things out of the U.S. and securing critical infrastructure. To give you an understanding of the security challenge we face in the United States, let me paint a picture of DHS operations.

Each year, Customs and Border Protection (CBP) admits approximately 420 million travelers– 88 million by air alone. In any given day, the Transportation Security Administration (TSA) screens over 2 million passengers using our domestic U.S. aviation system; and we rely on state and local partners to patrol surface transport, which handles traveler volumes that far exceed these levels. Each year U.S. Citizenship and Immigration Services (USCIS) processes nearly 7 million immigration benefits applications and petitions for foreign nationals. How do we effectively process travelers and applicants while identifying those among them who present a threat? More specifically, how do we deter or intercept terrorists who are willing to die for their cause – and how do we do that without unduly impacting on the lives of everyone else or bringing trade and travel to a screeching halt?

The National Commission on Terrorist Attacks Upon the United States, also known as the 9-11 Commission, pressed the importance of secure identification documents that can be verified in the screening process. "[S]ources of identification are the last opportunity to ensure that people are who they say they are and to check whether they are terrorists."

"For terrorists, travel documents are as important as weapons." Indeed, when we investigated the 9/11 attacks, we discovered that 18 of the 19 perpetrators had been issued U.S. identification documents and that some of these documents had been obtained fraudulently.

The need for secure identification is clear, but how should we determine what level of identity assurance is appropriate for a given encounter? Should biometrics be collected? Must the document be electronically verifiable?

Mission and Business Case Must Drive Technology Decisions

The business process and needs of our screening efforts must drive the technology choices that we make for our secure identification programs. We are fortunate to have many technology options today to choose from. These technologies supports our ability to: establish and verify the identity of individuals, both at time of enrollment and at subsequent encounters; conduct vetting appropriate to determine eligibility and assess risk for the specific program, including conducting checks against the Terrorist Screening Database (TSDB); assess validity of documents presented, as well as using physical security features to ensure documents are tamper-resistant. It is important to understand that, because the vetting conducted by DHS in a given program is based on the requirements of the program, an individual who has successfully completed a background check for one type of credential cannot be automatically qualified for other credentials if the vetting for that program is more stringent.

DHS is currently developing and implementing a number of high profile screening programs in which secure identification credentials figure prominently. As DHS develops the path for these programs, it creates its business case, unique to that program. This business case includes: the use case or business process desired; analysis of the environment in which the process will occur; the requirements established by the enabling legislation and the authority for the program; the overall mission of the implementing organization as well as DHS as a whole; the risks associated with the process or program; and mechanisms to ensure the protection of privacy and civil rights concerns.

While recognizing the individual challenges and environments, we must also identify opportunities to harmonize and enhance screening processes across DHS programs and rationalize and prioritize investments in screening technologies and systems. DHS has adopted the following principles to guide development of screening programs, where appropriate.

- 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 correct information held about them.

While one size does not fit all, neither does every program have to reinvent the wheel.

The following programs provide examples to illustrate how different the technology solutions can, and should, be when they are chosen to respond to business needs.

Western Hemisphere Travel Initiative (WHTI)
The institution of a travel document requirement and the standardization of travel documents are critical steps to securing our Nation's borders and increasing the facilitation of legitimate travelers. Currently, travelers at our land and sea ports of entry may present any of 8 thousand documents to CBP officers when seeking admission to the United States.

Our layered security strategy involves identifying and interdicting terrorists as early as possible – if not before they enter our country, then at the port of entry. Through its requirement that individuals carry a passport or other acceptable secure document to denote identity and citizenship, WHTI will greatly reduce the opportunities for fraud or misrepresentation of one's identity.

DHS has proposed accepting the cards associated with the existing trusted traveler programs, NEXUS, SENTRI, and FAST, and expanding the use of the facilitative technology already in use in these programs, vicinity Radio Frequency Identification (RFID), to other documents. This technology allows a unique card identifier to be read as the driver approaches the inspection booth, and the record associated in the system with that card is presented for the CBP Officer. The Department of State's Passport Card, currently under development, will also use vicinity RFID technology to meet DHS' operational needs at ports of entry. NIST certified the card architecture of the passport card as required in the FY 2007 DHS Appropriations Act.

Speeding up the document querying and authentication process gives more time for our CBP officers to ask questions and conduct inspections of those who require more scrutiny. Precious time now spent examining the face of a document will, instead, be used to interview higher risk individuals seeking to enter the U.S. We believe that with more people having secure documents and using this technology, WHTI will improve traffic flow at the border.

Because these documents will be used by DHS to determine eligibility to enter the U.S., and can directly interact with DHS systems, we can minimize the information on the document and rely instead on the information contained in DHS systems to verify that the person presenting the document is the one to whom it was issued.

In contrast, the business process associated with the Transportation Worker Identification Credential (TWIC), and the environment in which it's used, differs significantly.

Transportation Worker Identification Card (TWIC)

In furtherance of securing our seaports, the TWIC is a DHS screening initiative with joint participation from the TSA and the U.S. Coast Guard. The TWIC program, which began its roll out this week, provides a tamper-resistant biometric credential to maritime workers requiring unescorted access to secure areas of port facilities and vessels regulated under the Maritime Transportation Security Act of 2002. National deployment of the TWIC program will enhance security of ports by requiring credentialed merchant mariners and workers with unescorted access to secure areas of vessels and facilities to undergo a complete security threat assessment, which includes a fingerprint-based criminal history records check, and receive a TWIC.

In the future, port facility and vessel owners and operators will be required to integrate TWIC into their existing access control systems and operations. This second phase of the program will implement card reader requirements through rulemaking to verify the identity of workers entering secure areas by matching their fingerprint with the fingerprint template stored on their TWIC. Before implementing these requirements, DHS will conduct pilot tests in accordance with the SAFE Port Act, and the public will be afforded ample opportunity to comment on that aspect of the TWIC program through the rulemaking process.

The TWIC is intended to be used in a highly decentralized environment for biometric-based automated access control. Because of this, personally identifiable information must be included on the card that allows the reader technology, without human intervention, to make the determination as to whether the person presenting the document is the one to whom it was issued and whether the card is currently valid. In this program, decision-making for initial or continued eligibility, as well as issuance of the TWIC document, is centralized and determined through human review. The environment in which the TWIC is used, however, is decentralized and automated.

In a third contrast, the business process associated with the REAL ID program provides another aspect of this discussion.

REAL ID

During the terrorist attacks on the United States on September 11, 2001, all but one of the terrorist hijackers acquired some form of identification document, and used these forms of identification to assist them in boarding commercial flights, renting cars, and other necessary activities leading up to the attacks.

In response to the 9/11 Commission's recommendations, in May 2005, Congress enacted the REAL ID Act. The REAL ID Act directs DHS to establish certain minimum standards that States must adopt for State issued driver's licenses and identification cards intended for use for Federal official purposes, including access to federal facilities,

boarding Federally-regulated commercial aircraft, entry into nuclear power plants, and such other purposes as established by the Secretary of Homeland Security.

It is important to reiterate that this program will establish a set of minimum standards. The role of the Federal government in this case is to ensure commonality of approach, which includes minimum physical security features as well as quality and integrity of the issuance process, because of the role driver's licenses play in the U.S. as a core identity document. At the same time, we recognize that individual States have a strong and continuing interest in ensuring that these documents meet their primary purpose – the ability for the State to ensure and enhance driver safety.

Identification documents complying with the REAL ID Act are intended to be issued and used in a highly decentralized environment, with a variety of different users and business processes. Many of the users may not have rapid and easy access to automation from which to verify the authenticity of the document or verify that the person who presents the document is the one to whom it was issued. In this program, State driver's license eligibility determinations are informed and supported by electronic verification of the supporting documentation presented by the applicant with the agency who issued it. Use and validity of the document remains highly decentralized and usually requires human verification at the point where an individual is using a REAL ID driver's license or identification card as an identity document.

Privacy Considerations

In leveraging technologies for border security and facilitation of legitimate global travel, DHS has institutionalized the need to protect privacy, and 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 conducts periodic audits of its systems to ensure appropriate use. In addition, DHS provides notice regarding how information collected will be used and shared with outside entities, and how the information will be securely stored. DHS also provides notice to the individuals who participate in the programs as to the objectives and benefits of the program, as well as the privacy risks. These are the privacy principles that provide the opportunity for informed consent.

Analysis of risks to privacy and the manner in which those risks can be mitigated also plays a key role in determining which technologies will be used, and how, for a given mission. For example, the business case for WHTI documents the need for CBP to rapidly verify that the person presenting the document is the one to whom it was issued, that the document is valid, and to use information about that person to conduct appropriate checks. Vicinity RFID was selected as the technology best able to meet these requirements, because of its ability to be read at a distance and without close interaction with the card holder. DHS assessed the privacy risks associated with vicinity RFID, and has made technology choices to mitigate those risks. The vicinity RFID on the WHTI compliant document will only transmit a randomly assigned number to CBP's systems, and will not include any personally identifiable information. CBP's systems will then provide the information needed about the person to the officer for the encounter. This

mitigates the risk that an unauthorized person would intercept the RFID transmission and obtain meaningful information. The privacy risks were similarly assessed and mitigated in the implementation choices for the technology selected for the TWIC and REAL ID programs.

Physical Document Security Requirements

Physical security features are required on secure identification documents so the document can be used for its intended purpose when electronic verification systems are not available. Documents must be made physically secure using layered multiple security features, such as holograms, kinegrams, specialized inks, laser etching, and new security printing techniques specifically designed to thwart attempts to counterfeit or alter the documents.

To maintain a high level of physical document security, both to allow for secure processes and to protect the privacy of the individual, document producers and those who issue legitimate documents are in a constant battle to develop new production methods and security features to make the identification documents they issue more secure. However, technological advances have made commercial-quality scanning and printing equipment and processes widely available to the individual consumer. The availability of commercial-quality scanning and printing equipment and processes has significantly increased the quality of fraudulent documents encountered by all levels of law enforcement and government agency personnel.

It is for these reasons that access, travel, and identity documents must be continually reviewed and updated. The documents must incorporate advances in production technology and security features specially designed to thwart reproduction by scanners or other digital equipment. These investments will produce documents that are more tamper-resistant and therefore more secure. The development, production, and distribution of quality physically secure documents will be expensive, as it will require replacing old document production systems and infrastructure; however, the investment will pay healthy dividends in the security of this country.

Summary

These examples demonstrate the rationale for advocating a process whereby the business needs drive the technology appropriate for a specific use environment. I would like to also underscore how important it is that the DHS, charged with implementing these programs, continue to have the flexibility to analyze the program's requirements, and select the technology that best meets the needs of the environment. Mandates to use a specific technology would not permit DHS to utilize the most appropriate approach for a given mission, and would restrict our ability to evolve that approach in response to changing threats. This does not mean that DHS believes that every program should use a different technology solution. DHS is moving to standardize to a select few solutions, appropriate to the environments in which they will be used and the mission need of the program.

Mr. Chairman, thank you again for the opportunity to testify today. I am happy to respond to the Subcommittee's questions.