OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

STATEMENT OF CHARLES K. EDWARDS

ACTING INSPECTOR GENERAL

U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE THE

SUBCOMMITTEE ON BORDER AND MARITIME SECURITY

COMMITTEE ON HOMELAND SECURITY

U.S. HOUSE OF REPRESENTATIVES

September 11, 2012

Good morning Chairman Miller, Vice Chairman Quayle, Ranking Member Cuellar, and distinguished members of the subcommittee. I am Charles K. Edwards, Acting Inspector General of the Department of Homeland Security (DHS). Thank you for inviting me to testify about the results of our work on border security. I will present the results of three recent reports on DHS' implementation—along with other departments and agencies—of various programs aimed at securing our border and preventing terrorist travel.[1] Specifically, I will address: 1) DHS screening of foreign nationals, as well as the cooperation, resources, and technology necessary to share information and safeguard our borders; 2) the United States Visitor and Immigrant Status Indicator Technology Office's (US-VISIT's) oversight of biographic and biometric data for foreign nationals entering the United States; and 3) the Transportation Security Administration's (TSA's) implementation of the Secure Flight program.

Multiple Departments and Agencies Play Crucial Roles in Border Security

The security infrastructure at U.S. borders is layered and the Department of State (State), DHS components, and other Federal, state, local, tribal, and private entities play critical roles in securing our border. For example, State Department consular personnel review the visa applications of all individuals traveling to the United States from

[1] The information provided in this testimony is contained in the following reports: Information Sharing on Foreign Nationals: Border Security (OIG-12-39); US-VISIT Faces Challenges in Identifying and Reporting Multiple Biographic Identities (OIG-12-111); and Implementation and Coordination of TSA's Secure Flight Program (OIG-12-94).

countries where visas are required. State approves visas only after checking the individual's fingerprints against previous biographic records associated with those fingerprints to ensure that the individual has not previously used different biographic information to enter the United States. TSA performs passenger watchlist matching for all covered flights into, out of, within, and over the United States. U.S. Customs and Border Protection (CBP) analyzes cargo and passenger manifests to identify higher risk matters for subsequent examination, and CBP immigration Advisors provide real-time assistance to foreign authorities at some foreign airports.

In addition to control procedures that occur prior to foreign nationals entering the United States, other Federal entities have control procedures designed to identify potential criminal behavior at entry to the United States or subsequently, in order to flag individuals for future apprehension. CBP officers at ports of entry check travel documents to identify potential fraudulent or stolen passports, visas, or other travel documents before admitting an individual to enter the United States. Even after entry, US-VISIT and other DHS data systems play a crucial role in processing data captured by numerous agencies to identify and flag potential identity fraud or individuals who have overstayed their visas. Multiple layers of effective security programs and coordination among agencies are crucial to protecting our nation.

Screening of Foreign Nationals and Information Sharing[2]

We identified resource and technological difficulties facing DHS' border security programs in screening foreign nationals, as well as challenges in coordinating among DHS components.

Resource and technological difficulties: DHS officers at any of the 327 air, sea, or land border ports of entry have to access as many as 17 different DHS systems to verify the identity and evaluate the admissibility of foreign nationals seeking to enter the United States. This process is labor-intensive, and the inefficiency of using multiple data systems hinders border security officers in their efforts to verify or eliminate links to possible terrorism or other derogatory information. While CBP and U.S. Immigration and Customs Enforcement (ICE) have developed more streamlined software to conduct immigration inspections, apprehension, and enforcement, DHS officers with more complex border security caseloads still face challenges in data systems. In addition, some ports of entry, land, and maritime border operations had unmet infrastructure needs. For example, at some land border ports of entry, limited direct access to law enforcement, intelligence, and immigration databases and high-speed Internet connections had a negative effect on the operations of these locations. Some CBP Officers who conduct outbound screening – and most Border Patrol Agents in the field –

[2] Information Sharing on Foreign Nationals: Border Security (OIG-12-39).

use only mobile devices that lack the bandwidth and access to multiple databases that desktop terminals provide.

Information Sharing and Coordination: Our Inspection Report 12-39 describes challenges presented by the long-standing mission overlap between CBP and ICE agents at the northern border. The intersection of their responsibilities, along with inadequate information sharing, has sometimes led to duplication of missions and concerns over officer safety. These problems also hindered the effectiveness and efficiency of operations to screen and process foreign nationals. We determined that CBP and ICE do not always share all information and intelligence related to open investigations, even when the origin of the investigation comes from both agencies. Further, the data systems used by CBP and ICE are not designed for information sharing on investigations, or to identify operations that may overlap between the two agencies. DHS-level guidance is necessary to provide clarity on missions and priorities for law enforcement agencies that share overlapping mandates, such as ICE and CBP.

US-VISIT's Oversight of Traveler Data[3]

The Automated Biometrics Identification System (IDENT) maintained by US-VISIT contains hundreds of thousands of discrepant records. We also determined that the identity resolution processes at US-VISIT are manual and not specifically targeted to

[3] US-VISIT Faces Challenges in Identifying and Reporting Multiple Biographic Identities (OIG-12-111).

identifying individuals who may have presented fraudulent identities to attempt to enter the United States.

IDENT contains biographic and biometrics information collected by various agencies including State, ICE, CBP, U.S. Customs and Immigration Services (USCIS), and the Federal Bureau of Investigations (FBI). Each time an international traveler passes through a United States port of entry, US-VISIT checks the person's biometrics, i.e., fingerprint and/or picture, against a biometric watch list of more than 6.4 million known or suspected terrorists, criminals, and immigration violators. In addition, US-VISIT checks the foreign visitor's fingerprint along with their permit and/or other documents against a number of systems to verify an individual's identity and authenticate travel document. These efforts at US-VISIT assist CBP officers make a final determination as to whether the individual should be admitted.

Oversight of Overstays and Identity Resolution: According to US-VISIT officials, they have identified individuals who have overstayed visas by comparing visa information against entry and departure data, and established overstay lookouts so CBP officers and Department of State personnel can be warned of potential overstays seeking reentry to the United States. In fiscal year 2011, US-VISIT referred more than 900 visa overstay leads per week to ICE. US-VISIT also provides other Federal law enforcement and

Intelligence Community with historical biographic and biometric information in the course of their investigations.

With respect to identity resolution, US-VISIT reviews records of foreign nationals entering and exiting the United States where different biographic data were associated with the same biometrics. This process involves US-VISIT analysts manually reviewing entry records to determine whether biographic information was input incorrectly at the point of collection, or whether fraud may have occurred. For example, analysis of discrepant data may reveal that a husband and wife had their passports switched during entry, a traveler's first and last name was switched at entry, or a traveler's birth date was recorded using different day and month format.

Procedures Targeting Potential Identity Fraud Needs Improvements: The manual review process presents challenges considering the large volume of data that exist on travelers who sought entries into the United States. Specifically, our analysis of data from IDENT identified more than 800,000 instances affecting 375,000 individuals where the name and/or date of birth did not match other records with the same fingerprint identification number. These hundreds of thousands of records with inconsistent biographic data limit the effectiveness and efficiency of using biometrics to identify and prevent the use of fraudulent identities at U.S. ports of entry. According to US-VISIT officials, US-VISIT manually reviews IDENT encounters with multiple biographic records to identify

potential identity fraud. However, US-VISIT's current identity resolution effort is not designed to specifically target individuals who are using multiple identities to enter the United States. Since 2005, US-VISIT analysts have referred only two instances of biographic fraud to ICE.

Data Inconsistencies Hinder Oversight Effectiveness: Most of the multiple identities appear to be data integrity errors. For example,

- Test data existed in the alien encounter information that US-VISIT provided to us. In a number of instances, we reviewed records with the same fingerprint number but with fictitious names such as "Mickey Mouse" and "Jarvis Sample."
- In a number of instances, the same set of fingerprints was used to record the names of as many as seven different individuals.
- Nearly 400,000 records for women have different last names for the same first name, date of birth, and fingerprint. According to US-VISIT officials, these instances are likely women who changed their names after a marriage.

However, US-VISIT was unable to quantify how much of the biometric/biographic inconsistencies can be attributed to data entry and other identifiable errors, and how much occurred because of intentional fraud by individuals who used different biographical data to attempt illegal entry.

Examples of potential fraud: Our analysis of IDENT identified that individuals used different biographic information at ports of entry after they had applied for a visa under a different name or been identified as a recidivist alien. These multiple biographic identities were not flagged in IDENT. For example,

- A male who used two different names and dates of birth to attempt to enter the United States in 2008 and 2011 was identified as a repeated criminal (recidivist) alien.
- A female who was identified as a recidivist alien in 2008 used different biographic data to attempt to enter the United States, once in 2009 and twice in 2011.
- A female who was identified as a recidivist alien in 2006 attempted to enter the country on three visits in 2009, 2010, and 2011 under variations of the same name.

Although the more than 800,000 instances represented less than one percent of overall IDENT encounter data we received from US-VISIT, the potential risk can be significant. Critical work performed by CBP and State mitigates some of the security risks. However, without a process to distinguish between errors and potential fraud quickly, US-VISIT is limited in its ability to flag identity fraud, and therefore help border enforcement agencies prevent improper entries into the United States.

TSA's Implementation of the Secure Flight Program[4]

Through the Secure Flight program, TSA assumed from commercial operators the performance of passenger watchlist matching for all covered flights into, out of, within, and over the United States. Aircraft operators are required to submit passenger data to Secure Flight prior to flight departure for advanced passenger prescreening. Secure Flight implementation has resulted in a more consistent watchlist matching process. However, DHS and aircraft operator system outages sometimes disrupt the process.

More Consistent Watchlist Matching: TSA requires aircraft operators to transmit airline passenger information including name, gender, passport number [if applicable] and date of birth to Secure Flight. Passenger information is submitted 72 hours prior to flight departure, and a high priority queue has been established for reservations created subsequently. TSA matches the passengers' biographic information against the Terrorist Screening Database and the No Fly and Selectee subsets. If the information matches closely enough against a watchlist record, the Secure Flight system flags the record for manual review by a TSA analyst. If the analyst needs more information, the boarding pass is "inhibited' – it cannot be printed until the passenger provides identification to the aircraft operator and TSA. Based on the review, TSA may clear the individual.

[4] Implementation and Coordination of TSA's Secure Flight Program (OIG-12-94).

Alternatively, TSA may provide for additional screening at a security checkpoint, or deny boarding or authorization to enter a U.S. airport's sterile area.

Because all airlines are required to use the same process, Secure Flight has provided a more consistent watchlist matching process for both TSA and passengers. However, aircraft operators have the ability to override inhibited boarding passes. When this occurs, inhibited individuals who have not yet been cleared by Secure Flight may not be handled appropriately before entering an airport's sterile area or boarding an aircraft. In its response to our report, TSA said that they have taken steps to identify how and when aircraft operators inappropriately engaged in overrides, ensure screening is performed when overrides are identified, and launch compliance investigations.

Secure Flight Sometimes Disrupted by System Failures: Secure Flight's watchlist matching results are sometimes disrupted by DHS and aircraft operator system outages. Outages may require aircraft operators to revert to alternative procedures that may include pre-Secure Flight watch list matching procedures and protocols. TSA has established procedures to identify and resolve outages. Secure Flight has also taken steps to address these disruptions through operation center and system redundancy.

Our reports have described the work and coordination of agencies within and outside the Department of Homeland Security that play an important role in deterring terrorist

travel. Because of the hard work of these entities, we have identified and stopped terrorist acts before they have occurred. However, our reports have also identified a number of areas, including identification of fraudulent identities, system interfaces, and increased coordination, where agencies can make further improvements to help ensure the efficiency, accuracy, and effectiveness of our complex border security system.

Madam Chair, this concludes my prepared remarks. I welcome any questions that you or the Members of the Subcommittee may have.