

TESTIMONY OF
THOMAS WINKOWSKI
ASSISTANT COMMISSIONER
OFFICE OF FIELD OPERATIONS
U.S. CUSTOMS AND BORDER PROTECTION
U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE

HOUSE HOMELAND SECURITY COMMITTEE
SUBCOMMITTEE ON BORDER AND MARITIME SECURITY

SEPTEMBER 13, 2011

Chairman Miller, Ranking Member Cuellar, and distinguished Members of the Subcommittee, thank you for the opportunity to appear today to discuss the good work of U.S. Customs and Border Protection (CBP) related to ensuring and enforcing security measures implemented since the attacks of September 11, 2001. I appreciate the Committee's leadership and your commitment to helping ensure the security of the American people.

CBP's Role in Multiple Layers of Defense

CBP and, more broadly, Department of Homeland Security (DHS) continually refine our risk-based and layered approach to security, focusing our resources on the greatest vulnerabilities, extending our borders outward, and interdicting threats before they reach the United States. DHS, in cooperation with our interagency and foreign partners, is now screening people and goods earlier in the travel process. With more advanced and better quality data than ever before, we now employ an extensive network of research and analysis well before a traveler applies for admission at a U.S. port of entry.

Depending on the traveler's point of origin and travel and entry document requirements, the screening process can begin in a number of ways: with the application for a visa, application for electronic travel authorization, purchase of an airline ticket, or arrival at a foreign airport or domestic port of entry. At each step along the way, CBP, in

cooperation with other government agencies and commercial carriers, reviews information about the traveler, including their documents, their effects, and/or their responses to questions, prior to arrival at a U.S. port of entry. Several federal agencies are responsible for different aspects of our aviation security, while other countries and the private sector – particularly the air carriers – also have important roles to play. These multiple layers of defense across departments and agencies secure the aviation sector and ensure the safety of the traveling public.

The foiled plot to bring liquid explosives onboard U.S.-bound flights from the United Kingdom in 2006, the attempted bombing of Northwest Flight 253 on December 25, 2009, the failed Times Square bombing in May 2010, and the attempts to mail explosive devices within printer cartridges from Yemen in October 2010 are all powerful illustrations that terrorists continue to try to overcome security measures we have enacted since September 11, 2001.

CBP continually evaluates and supplements existing security measures with additional enhancements to strengthen our ability to identify and prevent the international travel of mala fide travelers and cargo. The success of these additional security measures depends in great part on our ability to gather, share and respond to information in a timely manner – using both strategic intelligence to identify existing and emerging threat streams, and tactical intelligence to perform link analysis and targeted responses.

CBP and Intelligence

As part of our efforts to screen passengers bound for the United States, CBP uses the U.S. Government's consolidated terrorist watchlist, specifically, the Terrorist Screening Database (TSDB), managed by the Terrorist Screening Center. In addition, we use additional relevant information from the Intelligence Community to determine whether someone may be a risk to a flight, requires further screening and investigation, should not be admitted, or should be referred to appropriate law enforcement personnel.

Further, CBP's Office of Intelligence and Investigative Liaison (OIIL), which serves as the situational awareness hub for CBP, provides timely and relevant information along with actionable intelligence to operators and decision-makers and improving coordination of CBP-wide operations. Through prioritization and mitigation

of emerging threats, risks and vulnerabilities, OIIL helps CBP to better function as an intelligence-driven operational organization and turns numerous data points and intelligence into actionable information for CBP officers and analysts.

National Targeting Center

The National Targeting Center (NTC) is another key tool for DHS in analyzing, assessing, and making determinations based on the TSDB and other intelligence information. The NTC is a 24/7 operation, established to provide tactical targeting information aimed at interdicting terrorists, criminal actors and contraband at the earliest point. CBP's Automated Targeting System (ATS) is a decision-support tool crucial to the operation of the NTC and is a primary platform used by DHS to match travelers, conveyances, and shipments against law enforcement information and known patterns of illicit activity.

Safeguards for Visas and Travel

One of the initial layers of defense in securing air travel is preventing dangerous persons from obtaining visas, travel authorizations and boarding passes. Before boarding a flight destined for the U.S. or arriving at a U.S. port of entry, most foreign nationals need to obtain a visa – issued by a U.S. embassy or consulate – or, if they are eligible to travel under the Visa Waiver Program (VWP), they must apply for a travel authorization issued through the Electronic System for Travel Authorization (ESTA).¹

The Department of State (DOS) is responsible for visa issuance. DOS also screens all visa applicants' biographic data against the DOS Consular Lookout and Support System, which includes entries that alert consular officers to the existence of TSDB files, for records related to potential visa ineligibilities and checks their biometric data (i.e., fingerprints and facial images) against other U.S. Government databases for records indicating potential security, criminal and immigration violations prior to the issuance of the visa. For individuals traveling under the VWP, CBP operates ESTA, a

¹ Exceptions would be citizens of countries under other visa exempt authority, such as Canada. Citizens of countries under visa exempt authority entering the U.S. via air are subjected to CBP's screening and inspection processes prior to departure. In the land environment, they are subjected to CBP processing upon arrival at a U.S. port of entry.

web-based system through which individuals must apply for travel authorization prior to traveling to the United States. Through ESTA, CBP conducts enhanced vetting of VWP applicants in advance of travel to the United States in order to assess whether they could pose a risk to the United States or the public at large. Additionally, through interactive communications with CBP, air carriers are required to verify that VWP travelers have a valid authorization before boarding an aircraft bound for the United States.

Pre-departure Vetting

CBP can also gather information and assess risk at the point of travel booking. CBP conducts pre-departure and outbound screening for all international flights arriving into and departing from the United States. This works in concert with the Transportation Security Administration's Secure Flight program, which vets 100 percent of passengers flying to, from, and within the U.S against the No Fly and Selectee portions of the known or suspected terrorist watch list, or TSDB. The NTC uses a variety of data sources and automated enforcement tools to perform its function. The process starts when a traveler purchases a ticket for travel to the United States; a Passenger Name Record (PNR) may be generated in the airline's reservation system. PNR data contains various elements, including information on itinerary, co-travelers, changes to the reservation, and payment information. CBP receives PNR data from the airline at various intervals beginning 72 hours prior to departure and concluding at the scheduled departure time.

CBP uses the Automated Targeting System (ATS) to then evaluate the PNR data against "targeting rules" that are based on law enforcement data, intelligence information and past case experience. ATS allows CBP to identify and interdict travelers with potential nexus to transnational crime, including terrorism, narcotics trafficking, and human smuggling.

The traveler's check-in provides the next opportunity in the travel process for CBP to gather information and assess risk. On the day of departure, when an individual checks in for his or her intended flight, the basic biographic information from the individual's passport is collected by the air carrier and submitted to CBP's Advance Passenger Information System (APIS). Carriers are required to verify the APIS against the traveler's government issued travel document and provide the data to DHS at least 30

minutes before departure, or up to the time of securing the doors if using APIS Quick Query, for all passengers and crew on board.² APIS data contains important identifying information that is not included in PNR data, including verified identity and travel document information such as a traveler's date of birth, citizenship, and travel document number. DHS vets APIS information on all international flights to and from the United States against the TSDB, as well as against criminal history information, records of lost or stolen passports, public health records, and prior immigration or customs violations and visa refusals. APIS is also connected to Interpol's lost and stolen travel document database for routine queries on all foreign passports used for check-in.

Another layer in the vetting process is the Immigration Advisory Program (IAP), which stations CBP officers at eight foreign airports in six countries in coordination with the host foreign governments. Officers are deployed to these key transit hubs and work with border control authorities, foreign law enforcement agencies and air carriers to identify known or suspected terrorists and other high risk travelers and assist in preventing them from boarding aircraft destined for the United States. CBP officials at the NTC support IAP by screening all travelers against the TSDB, including the subset No Fly list, ESTA denials, visa revocations, public health lookouts, lost and stolen passport records, and all State Department records for persons identified as actually, or likely, having engaged in terrorist activity. At IAP locations, CBP officers can make "no board" recommendations to carriers and host governments regarding passengers bound for the United States who may constitute security risks, but officers do not have the authority to arrest, detain, search or prevent passengers from boarding planes. Those authorities lie with the host government.

After the attempted bombing on December 25, 2009, CBP expanded on the NTC's IAP pre-departure screening efforts to include screening at all foreign airports with direct flights departing to the United States to identify and assess risks prior to travel and prevent the boarding of high-risk travelers. When pre-departure screening identifies a potential high risk traveler, the NTC confirms the information through vetting procedures, and then coordinates the issuance of "no board" recommendations to carriers

² APIS is the electronic data interchange for air carrier transmissions of electronic passenger, crew member and non-crew member manifest data.

via the nearest ICE or CBP Attaché, Air Carrier Security Office, and the CBP Regional Carrier Liaison Group. Now, as a result of these efforts, 100 percent of travelers on all flights arriving at and departing from the U.S. are checked against government databases prior to boarding a flight. During fiscal year 2011 to date, pre-departure screening by the NTC has kept more than 2,000 high-risk or otherwise inadmissible travelers from boarding flights destined for the United States.

In March 2010, the NTC implemented a new program to conduct continuous vetting of U.S. nonimmigrant visas that have been recently issued, revoked and/or denied. The continuous vetting ensures that changes in a traveler's visa status are identified in near real-time, allowing CBP to immediately determine whether to provide a "no board" recommendation to a carrier or recommend that DOS revoke the visa, or whether additional notification should take place for individuals determined to be within the United States. If a violation is discovered, and the person is scheduled to travel to the U.S., CBP will request that DOS revoke the visa and recommend that the airline not board the passenger. If no imminent travel is identified, and derogatory information exists that would render a subject inadmissible, CBP will coordinate with DOS for a prudential visa revocation. If the subject of an existing visa revocation initiated by the DOS or recommended by CBP is found to be in the United States, CBP will notify the ICE Counterterrorism and Criminal Exploitation Enforcement Unit for further action as appropriate.

Additionally, ICE has co-located Visa Security Program (VSP) personnel at the NTC to augment and expand current operations. ICE special agents and intelligence analysts conduct thorough analysis and in-depth investigations of high-risk visa applicants. The focus of the VSP and NTC are complementary: the VSP is focused on identifying terrorists and criminal suspects and preventing them from exploiting the visa process and reaching the United States, while the NTC provides tactical targeting and analytical research in support of preventing terrorist and terrorist weapons from entering the United States. The co-location of VSP personnel at the NTC has helped increase both communication and information sharing.

Vetting while en route to the United States and upon arrival

While flights are en route to the United States, CBP continues to evaluate the updated APIS and PNR information submitted by the airlines. Based on the information garnered during the in-flight analysis, as well as the CBP officer's observations at the port of entry, a determination is made as to whether the traveler should be admitted to the United States following primary inspection or referred for a secondary inspection.

Conclusion

As this committee no doubt knows, we live in a world of ever-evolving risks, and we must move as deftly as possible to identify and fix security gaps and to anticipate future vulnerabilities. CBP will continue to work with our colleagues within DHS, and with DOS, and the Intelligence Community to address these challenges.

Chairman Miller, Ranking Member Cuellar, and members of the Subcommittee, thank you for this opportunity to testify. I look forward to answering your questions.