

TESTIMONY OF
KEVIN MCALEENAN
ACTING 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 11, 2012

Good morning Chairman Miller, Ranking Member Cuellar, and distinguished Members of the Subcommittee. Thank you for the opportunity to appear before you to represent U.S. Customs and Border Protection (CBP) and, on this solemn anniversary, to discuss our efforts to disrupt terrorist travel and promote travel security. I appreciate the Committee's leadership and your continued efforts to ensure the security of the American people.

CBP's Actions to Prevent Terrorist Travel

As the unified border security agency of the United States, CBP is responsible for securing our nation's borders while facilitating the flow of legitimate international travel and trade that is so vital to our Nation's economy. Within this broad responsibility, our priority mission remains to prevent terrorists and terrorist weapons from entering the United States.

To do this, CBP works in close partnership with the federal counterterrorism community, including law enforcement agencies, the intelligence community, U.S. Immigration and Customs Enforcement (ICE), the Transportation Security Administration (TSA), the Department of State, state and local law enforcement, the private sector, and our foreign counterparts to improve our ability to identify risks as early as possible in the travel continuum, and to implement security protocols for addressing potential threats. CBP works with its counterparts to apply its capabilities at multiple points in the travel cycle to increase security by receiving advance information, employing sophisticated targeting systems to detect risk, and acting through a global network to address risks or prevent the movement of identified threats toward the United States at the earliest possible point in their travel.

In concert with its partners, CBP strives to ensure that travelers who present a risk are appropriately interviewed or vetted before boarding a flight bound for the United States, and that any document deficiencies are addressed before traveling to the United States. CBP has placed officers in strategic airports overseas to work with carriers and host nation authorities, and has built strong liaisons with airline representatives to improve our ability to address threats as early as possible and effectively expand our security efforts beyond the physical borders of the United States.

These efforts seek to keep our transportation sectors safe and prevent threats from ever reaching the United States. These efforts also enhance efficiency and create savings for the U.S. Government and the private sector by preventing inadmissible travelers from traveling to the United States.

Travel to the United States

Given that commercial air transportation remains the primary target of terrorist organizations seeking to attack the homeland or move operatives into the United States, my testimony will focus on international air travel. CBP inspects nearly one million travelers each day as they enter the United States, and about 30 percent--almost 100 million a year--of these travelers arrive via commercial aviation. CBP has developed and strategically deployed resources to detect, assess and, if necessary, mitigate the risk posed by travelers throughout the international travel continuum. CBP and its partners work to address risk at each stage in the process: (1) the time of application to travel; (2) ticket purchase or reservation; (3) check in at a foreign airport; and (4) arrival in the United States. Aspects of this strategy are highlighted below.

Application to Travel

In general, most non-U.S. citizens wishing to travel to the United States need to either apply for a visa from the Department of State (DOS) at a U.S. Embassy or Consulate, or a travel authorization from CBP via the Electronic System for Travel Authorization (ESTA). CBP plays an important role in each of these processes.

Non-Immigrant Visa Process

Travelers that require Non-Immigrant Visas (NIVs) to travel to the United States must apply to DOS to be a temporary visitor under specific visa categories, including those for business, pleasure, study, and employment-based purposes.

DOS manages the process of initially vetting visa applicants including biometric and biographic checks. DOS Consular Officers then adjudicate the visa application, which may include an interview of the applicant, to determine eligibility. Applicants suspected of committing fraud or suspected of other criminal or terrorist links are referred to DOS, or the appropriate agency, for additional investigation.

CBP operates and monitors the Visa Hot List, a tool to re-vet previously issued visas against lookout records, to identify persons whose eligibility for a visa or entry to the United States has changed since the issuance of that visa. Relevant information that is uncovered is passed to DOS, ICE, or other agencies as appropriate. This continuous re-vetting by CBP has resulted in the revocation of over more than 3,000 visas by DOS since its inception in March of 2010.

To further enhance visa screening efforts, ICE, CBP and DOS are collaborating on the development of an automated visa application screening process that will broaden the scope to identify potential derogatory information prior to visa adjudication and issuance, and synchronize reviews of the information across these agencies. This process may be used as a precursor to and in conjunction with the current DOS Security Advisory Opinion (SAO) and Advisory Opinion (AO) programs. The joint program will leverage the three agencies' expertise, authorities, and technologies, such as CBP's Automated Targeting System (ATS), to screen pre-adjudicated visa applications. It will significantly enhance the U.S. Government's anti-terrorism efforts, improving the existing process by extending our borders outward and denying high risk applicants the ability to travel to the United States.

Electronic System for Travel Authorization (ESTA)

Since 2009, travelers traveling to the United States by air or sea and intending to apply for admission under the Visa Waiver Program (VWP)¹, must first apply for travel authorization through CBP's online application system, the Electronic System for Travel Authorization (ESTA). Through this process, CBP incorporates targeting and database checks to identify those who are statutorily ineligible to enter the United States under the VWP and those who may pose a national security or criminal threat if allowed to travel. The majority of ESTA applications are approved; however, if derogatory information is revealed during the vetting process, the application is denied and the applicant is directed to DOS to initiate a formal visa application process. In Fiscal Year 2012 (through August 2012), CBP has vetted over 10.7 million ESTA applications and denied more than twenty-one thousand.

Ticket Purchase/Reservation

Passenger Name Record

As part of CBP's layered enforcement and risk segmentation approach, the next opportunity to review a traveler's information occurs upon the purchase of a ticket, when the carrier creates a Passenger Name Record (PNR). All commercial airlines are required to make their PNR systems and data available to CBP. The PNR is provided to CBP up to 72 hours in advance of travel, which permits CBP to conduct research and risk segmentation on all travelers including U.S. citizens and non-U.S. citizens. At this point, CBP, in cooperation with other government

¹ The 36 countries currently designated for participation in the Visa Waiver Program include: Andorra, Australia, Austria, Belgium, Brunei, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, South Korea, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Monaco, the Netherlands, New Zealand, Norway, Portugal, San Marino, Singapore, Slovakia, Slovenia, Spain, Sweden, Switzerland, and the United Kingdom.

agencies, begins a more comprehensive assessment of each traveler's risk by reviewing his/her travel documents, responses to questions on the ESTA or visa application, travel companions, and patterns of travel to identify those who may be ineligible to travel or who may warrant additional vetting.

Check-in

Advance Passenger Information System

Advance Passenger Information System (APIS) regulations require that carriers transmit all passenger and crew manifest information before departure, prior to securing the aircraft doors. APIS data includes the biographic traveler information that is found in a passport, such as a name and date of birth. APIS data also includes itinerary information, such as the date of travel and flight information. This information is used by CBP, in conjunction with the PNR data, to identify known or suspected threats before they depart the foreign location.

In 2007, CBP published the APIS Pre-Departure Final Rule, enabling CBP systems to conduct vetting prior to passengers gaining access to the aircraft or departing onboard a vessel. This regulation added an essential layer to our anti-terrorism security measures. As part of the implementation of the regulation, CBP developed an interactive communications functionality where carriers can transmit single-passenger APIS messages as passengers check-in and receive an automated response message.

As part of the Department of Homeland Security (DHS) commitment to establish a common reporting process for carriers submitting traveler information to DHS components, CBP and TSA aligned the CBP APIS Pre-Departure requirements with those of the TSA Secure Flight program,

so that air carriers transmit data once and receive a combined DHS response message that includes both the TSA Secure Flight screening results and the traveler's ESTA status. This consolidated information helps carriers make informed boarding decisions. CBP is currently expanding this capability to include a document validation check, to provide confirmation to the airlines that the individual's visa is valid as well.

National Targeting Center

CBP leverages all available advance passenger data including the PNR and APIS data, previous crossing information, intelligence, and law enforcement information, as well as open source information in its anti-terrorism efforts at the National Targeting Center (NTC). The NTC is a 24/7 operation that makes extensive use of intelligence materials and law enforcement data, allowing analysts and targeting officers to make tactical decisions at all points along the travel continuum. Starting with the earliest indications of potential travel, including United States-bound travel reservations, ESTA applications, visa applications, and passenger manifests, and continuing through the inspection or arrivals process, the NTC is continually analyzing information gleaned from these sources using CBP's Automated Targeting System (ATS). ATS is a decision-support tool for CBP officers which compares information on travelers arriving in, transiting through, and exiting the country against law enforcement and intelligence databases to identify individuals requiring additional scrutiny. This information is also matched against targeting rules developed by subject matter experts. Targeting rules are based on actionable intelligence derived from current Intelligence Community reporting or other law enforcement information available to CBP.

NTC analyzes each traveler's risk before departure to identify possible matches to the U.S. Government's consolidated terrorist watchlist, Interpol lost and stolen passports, criminal activity, fraud, and other mala fide travelers, including U.S. citizens. Through direct networks with commercial airlines and connections to CBP officers overseas as part of the Immigration Advisory Program (IAP), NTC officials are able to issue no-board recommendations to the airline to keep suspected high-risk passengers from traveling to the United States. In FY 2011, NTC made 3,181 no board recommendations to carriers. In FY 2012 (through August 2012), there have been more than 3,600 no board recommendations. The NTC vetting process for international passengers continues while the flight is en route to the United States in order to identify any travelers who, although they may not be national security risks, may need to be referred for a more thorough inspection at the first port of entry upon arrival in the U.S. for other potential violations.

In addition to expanding the Nation's zone of security beyond the United States and improving operational efficiency, NTC pre-departure programs result in significant monetary savings by preventing inadmissible passengers from boarding flights destined to the United States, where upon arrival most of them likely would have to be processed by CBP for refusal or removal, generating detention costs for the U.S. Government and additional repatriation expenses for commercial carriers.

In a recent effort to make CBP passenger and cargo targeting more effective, the NTC was established as a stand-alone entity in the Office of Field Operations with greater responsibility for CBP passenger and cargo targeting operations at the port of entry. The NTC continues to improve its operations as DHS and CBP anti-terrorism targeting requirements expand by

exploring new and innovative ways to identify, interdict or deter terrorists, their weapons and their supporters.

Immigration Advisory Program

IAP is another integral component of CBP's layered security approach. With advance targeting support from the NTC, IAP officers work in partnership with foreign law enforcement officials, to identify and prevent terrorists and other high-risk passengers, and then work in coordination with commercial air carriers to prevent these individuals from boarding flights destined to the United States. Maximizing the use of new mobile technology to enhance on-site targeting, IAP officers conduct passenger interviews and assessments to evaluate the potential risks presented by non-watchlisted travelers. The IAP is currently operational at eleven airports in nine countries including Amsterdam, Doha, Frankfurt, London Heathrow and Gatwick, Madrid, Manchester, Mexico City, Panama City, Tokyo and Paris.

Since the inception of the program in 2004, IAP officers have been successful in preventing the boarding of more than 15,700 high-risk and improperly documented passengers, to include matches to the TSDB.

Arrival at a U.S. Port of Entry

Arrival Processing

Upon arrival in the United States, all persons are subject to inspection by CBP officers. Upon application for admission to the United States, this inspection begins with CBP officers scanning the traveler's entry document and performing a query of various CBP databases for exact or possible matches to existing lookouts, including those of other law enforcement agencies. The system queries the document information against the APIS manifest information previously received from the carrier and provides any enforcement information about the traveler to the officer for appropriate action. APIS data is verified for completeness and accuracy through this process.

For most foreign nationals arriving at U.S. airports, fingerprint biometrics and photographs are captured by CBP officers. If the traveler has been previously fingerprinted, either at time of visa application or during a previous trip to the United States, the newly captured fingerprints will be compared to the originals to ensure the fingerprints match. Once a verified identity is established, the system will identify any watchlist information and return the results to the officer for appropriate processing. If the traveler has not been previously fingerprinted, the officer will collect all ten fingerprints and a biometric watchlist search will be conducted, returning the search results to the officer. In addition to the biographic and biometric system queries performed, each traveler is interviewed by a CBP officer to determine the purpose and intent of their travel, and whether any further inspection is necessary based on concerns for national security, identity or admissibility, customs, or agriculture.

If upon review of the system queries there are any exact or possible matches to the TSDB, including potential matches to the “No Fly” List, or other law enforcement lookouts, the NTC will be notified and coordinate with the port of entry for appropriate disposition or action. Additionally, CBP has established a Counter-Terrorism Response (CTR) protocol at ports of entry for passengers arriving with possible links to terrorism. CTR protocol mandates immediate NTC notification, initiating coordination with the Terrorist Screening Center (TSC), the National Counter Terrorism Center (NCTC), ICE, and the Federal Bureau of Investigation (FBI) Terrorist Screening Operations Unit (TSOU) and National Joint Terrorism Task Force (NJTTF).

For CBP’s Preclearance locations in Aruba, Bermuda, the Bahamas, Canada, and Ireland, customs, agriculture, and immigration inspection and examination typically occurs at the Preclearance location instead of upon arrival in the United States. Therefore, this process allows the aircraft to arrive at a domestic airport gate in the United States and travelers may proceed to their final destination without further CBP processing; however, CBP may conduct further inspection or engage in enforcement action after a pre-cleared flight departing from a preclearance location arrives in the United States.

For CBP land border locations, the Western Hemisphere Travel Initiative (WHTI) implemented the first 9/11 Commission border security recommendation and legislative mandate by reducing the number of acceptable travel documents from more than 8,000 to a core set of six secure documents types which can be automatically queried via law enforcement databases as the vehicle approaches the CBP officer. Today, more than 16 million individuals have obtained Radio Frequency Identification (RFID) technology-enabled secure travel documents, which can be verified electronically in real-time back to the issuing authority, to establish identity and

citizenship. The implementation of WHTI in the land border environment, and the increased use of RFID-enabled secure travel documents, have allowed CBP to increase the national law enforcement query rate, including the terrorist watch list, to over 98 percent. By comparison, in 2005, CBP performed law enforcement queries in the land border environment for only five percent of travelers.

As of June 2009, all major land border ports, representing 95 percent of all inbound vehicle traffic, have been upgraded to include improved license plate readers, RFID readers and improved processing applications to facilitate the inspection of travelers and vehicles using the new RFID-enabled travel documents. Since June 2009, the average number of imposter apprehensions, counterfeit and altered documents seized has declined to 42 per day from 84 per day (a 50 percent decrease).

Outbound: Air, Land and Sea

In addition to vetting inbound flights for high-risk travelers, CBP also developed protocols to enhance outbound targeting efforts within ATS, with the goal of identifying travelers who warrant outbound inspection or apprehension. Outbound targeting programs identify potential matches to the TSDB, including potential matches to the “No Fly” List, as well as National Criminal Information Center fugitives, and subjects of active currency, narcotics and weapons investigations. Additionally, outbound operations are enhanced by the implementation of targeting rules designed to identify and interdict subjects with a possible nexus to terrorism or links to previously identified terrorist suspects. As with inbound targeting rules, outbound targeting rules are continually adjusted to identify and interdict subjects of interest based on current threat streams and intelligence. Advance outbound manifest information is also obtained

through the APIS system from carriers for all passengers 30 minutes prior to departure or if using the APIS Quick Query mode, then carriers can transmit in real time as each passenger checks in for the flight prior to boarding.

As soon as APIS information becomes available, prior to the departure of a commercial conveyance, CBP and the TSA immediately begin the screening and vetting processes of the outbound flight for possible inclusion in the TSDB, including potential matches to the “No Fly” and Selectee List, as well as other law enforcement lookouts, using any and all available biographic information of the traveler. CBP’s law enforcement capability and commitment to national security, through the monitoring and vetting of outbound flights, were highlighted on May 1, 2010 when CBP officers arrested Faisal SHAZAD as the man suspected in the Times Square car bomb plot as he attempted to flee the country on a flight destined to Dubai. SHAZAD had, hours before, come to the attention of Federal law enforcement authorities in part because of data collected by CBP. Later, when SHAZAD tried to flee the country by purchasing a ticket on his way to the airport, it was CBP’s collection of API data that alerted us to his presence on the flight for Dubai, enabling us to take him into custody before the plane departed. CBP’s capabilities were also evident in September 2009 when Najibullah ZAZI plotted an attack against the New York City subway system; in this case, CBP’s databases led to the identification of two of ZAZI’s previously unknown co-conspirators. One pled guilty in April 2010 and the other was found guilty on May 21, 2012. Also, in October 2009, David Coleman HEADLEY was arrested and pled guilty to plotting attacks in Copenhagen and conducting surveillance in support of the November 2008 attacks in Mumbai, India; CBP identified HEADLEY using partial name and travel routing provided by FBI.

Conclusion

CBP is committed to protecting our country from terrorists and terrorist weapons while ensuring safe international travel and facilitating legitimate trade. CBP is continually updating and adjusting our programs to enhance the overall efficiency of how we operate in this ever-changing global environment. As part of our mission, CBP fosters partnerships and encourages cooperation with the law enforcement community, industry and foreign governments. CBP has built a multilayered approach for screening and identifying potential travelers to the United States who may pose a threat to the homeland and will continue to use all means within our authority to protect the Nation and its citizens. Thank you for allowing me the opportunity to testify before you today, and I look forward to answering your questions.