Center for Immigration Studies

Backgrounder

August 2011

Border Watchlisting a Decade after 9/11

By Janice Kephart

Summary

The tedious process of watchlisting and making watchlists available to our frontline border and aviation operators is the most important tool our nation has to curtail attempted "legitimate" terrorist travel — meaning, those terrorists who seek to use our border and aviation system to enter the United States. The 9/11 Commission recommended significant changes to watchlisting, including merging 11 disparate watchlists into one base list. Today, this single list is simply termed the "Terrorist Watchlist." The entity recommended to accomplish this goal was, and now is, the National Counterterrorism Center (NCTC). The Commission's focus on watchlisting addresses — in part — findings of fact of missed watchlist opportunities of (at least) two 9/11 hijackers who were known to the CIA in March 2000, but whose entry into the United States was never communicated to the border, aviation, or other members of the intelligence community until August 24, 2001.

This *Backgrounder* seeks to provide a historical perspective on watchlisting since 9/11 as it relates to the border and aviation communities, clarify how watchlisting works, and provide findings of facts and recommendations to solve remaining issues. The goal is to help improve watchlisting to make it accurate, efficient, and thorough for the right customers in real time.

Findings

- The 9/11 Commission recommendations to consolidate terrorist watchlisting and the analytic institutions responsible for creating and maintaining the Terrorist Watchlist are, for the most part, implemented. The NCTC is responsible for creating the Terrorist Identities Data Mart (TIDE), while the Terrorist Screening Center, run by the FBI, culls and sorts for those individuals who meet a "reasonable suspicion" standard. These individuals are listed on the "Terrorist Watchlist." It is this list that feeds the more specific border and aviation watchlists to which traveler names are submitted to today.

- The pronounced example of the Christmas Day Bomber's ability to board a plane in 2009 with a still-valid U.S. visa despite being known to the intelligence community seemed, on the surface, to replicate the deep-seated problems with watchlisting — including the intelligence community's lack of information-sharing with the border and aviation frontline operators — related by the 9/11 Commission. That assumption is inaccurate; the authorities, relationships, and operations are in place to get watchlisting right. Instead, what is lacking are technology, clear standard operating procedures, and implementation of other 9/11 Commission recommendations. These gaps create vulnerabilities that widen quickly when multiplied out over vast quantities of data. The good news? We can fix them.

Recommendations

- To improve watchlisting, the intelligence community needs complete information access in real time. Privacy and security issues have kept the intelligence community from allowing analysts to acquire all source information across the foreign/domestic divide quickly and efficiently as highlighted by

Janice Kephart is the Director of National Security Policy at the Center for Immigration Studies.

the 9/11 Commission. The problem to date has been, in part, that technology to secure data on the one hand, and make sure users who need it have access to it, has been lacking. That is no longer the case. Technical solutions such as "cloud computing" and dynamic encryption keys are now available to store data together but protect it by source, type, and value, for example. These technical solutions need to be piloted and incorporated into NCTC and TSC operations as soon as possible. To ensure a more accurate watchlist, biometrics, including digitized facial images and fingerprints, need to be fully incorporated into watchlisting. A name-based system remains too easy to game, and too easy to misidentify legitimate travelers.

- "Person-centric" traveler histories were recommended by the 9/11 Commission and enacted into law, but still have not been implemented by the Department of Homeland Security. The travel and immigration histories of all foreign-born travelers, including biometrics, should be easily available for analysis by the NCTC and TSC. This will also allow foreign persons applying for benefits to have their information held over time, minimizing fraud on the one hand while easing processing of new benefits sought because information will not need to be re-populated, as caching now does for Internet websites. Where privacy issues exist, these can be written into the information-sharing rules up-front.

- Law enforcement data obtained from abroad by Immigration and Custom Enforcement Visa Security Units conducting terrorist investigations of visa applicants abroad need to be incorporated into watchlist analysis. Congress needs to prioritize the VSU expansion, and give DHS visa revocation authority.

- The United States must do what it can to keep European Union agreements in place pertaining to Passenger Name Records; these records are absolutely essential to assuring accuracy of matching watchlist information to relevant aviation travelers.

- All visa holders and visa waiver participants should have their information vetted at least every two years, and every time they seek to travel to the United States. Right now, visa waiver travelers are subject to higher security thresholds than many visa holders from countries not friendly to the United States. Applying a standardized approach avoids profiling, establishes security away from our borders, and enables real-time vetting where derogatory information develops after visa issuance. Eventually, with cloud technology, vetting could be done in real time, on a daily basis if necessary, for all visa holders.

While the 10-year anniversary of the September 11 attacks looms, the intelligence community continues to fill the gaps that remain in supporting the border law enforcement community in curbing terrorist travel. While some of this work is purely analytical and driven to produce reporting on such things as travel document methods and alien smuggling networks, the most operationally important is the support provided by the intelligence community in keeping terrorists from getting visas, getting on planes, crossing our borders illegally, or permitted entry into our country at our borders amongst the millions of legitimate travelers to the United States annually.

The foundation of all watchlisting is TIDE, the single, massive dumping ground of terrorist data, as indicated by its name, the Terrorist Identities Datamart Environment (TIDE). TIDE is the foundation today for all other federal watchlists, including the critical watchlists that support our border and aviation community. Thus TIDE's strength and accuracy are essential components to not only curtailing terrorist travel, but supporting our national security more generally. It is thus worthwhile to review the effectiveness of TIDE, and more broadly how we came to where we are today in watchlisting, where we need to go, and why.

TIDE Basics

TIDE consists of pockets of classified and unclassified data, domestic and foreign sources, as well as 17 countries with which the United States has terrorist watchlist-sharing agreements. Procedures for nominating a suspected terrorist for inclusion in TIDE are in place across the law enforcement community. Analysts at the National Counterterrorism Center (NCTC) do the initial cull of information on known or "reasonably suspected" terrorists (those who prepare or aid terrorism) and their associates.

Analysts sift, scrutinize, and make decisions on what names to include or remove from TIDE. The sifting process that takes place today is a complete replacement for the 11 ad hoc watchlists produced by nine separate agencies used throughout the law enforcement and intelligence communities prior to 9/11. Unfortunately, today they still must search separate Central Intelligence Agency (CIA) and Federal Bureau of Investigation (FBI) databases that are not commingled, even if they are available as needed. According to the TIDE fact sheet, "as of March 2011, TIDE contained more than 640,000 persons, but only about 500,000 separate 'identities' because of the use of aliases and name variants. U.S. Persons (including both citizens and legal permanent residents) make up less than 2 percent of the listings."[1]

TSD Basics

TIDE supplies the Terrorist Screening Center Database (TSD) with known terrorist names, deleting terrorist associates where no information points to actual support of terrorist activities. TSD is maintained by the FBI at the Terrorist Screening Center, which holds detailees from Transportation Security Administration (TSA), U.S. Customs and Border Protection (CBP), the State Department (State), and other agencies who help drill down and provide final adjudication as to what names are on, and off, the "Terror Watchlist." According to Terrorist Screening Center (TSC) Director Tim Healy, watchlist nominations are made as follows:

> "TSC accepts nominations into the Terrorist Watchlist when they satisfy two requirements. First, the biographic information associated with a nomination must contain sufficient identifying data so that a person being screened can be matched to or disassociated from a watchlisted terrorist. Second, the facts and circumstances pertaining to the nomination must meet the 'reasonable suspicion' standard of review established by terrorist screening Presidential Directives. Reasonable suspicion requires 'articulable' facts which, taken together with rational inferences, reasonably warrant a determination that an individual is known or suspected to be or has been engaged in conduct constituting, in preparation for, in aid of or related to terrorism and terrorist activities, and is based on the totality of the circumstances."[2]

This consolidated watchlist then is provided, en masse, to a host of customers: from cargo and international postal screeners to special events like the World Cup, to motor vehicle departments when issuing HAZMAT licenses, to gun shops for purchases, to state and local police officers during investigations, and to over 70 state and local intelligence fusion centers. Fusion centers now receive notices when encounters occur in their region or with a suspect in one of their cases. Select foreign partners receive some of the TSD watchlist as well.[3]

Terrorist Travel Watchlist Basics

The border niche watchlists support the differing requirements of each agency. The 11 pre-9/11 ad hoc watchlists were disparate, and a handful of them were in the border community.[4] Some were classified. Some were not. Today, the NCTC represents the intelligence community in nearly all things counterterrorism-related. The NCTC was recommended by the 9/11 Commission[5] and mandated by Homeland Security Presidential Directive (HSPD) 6.[6] It is the work of a couple hundred analysts at the NCTC to populate TIDE, which populates the TSD, which ultimately supports all three key border security-related databases.

These border databases are the Consular Lookout and Support System (CLASS)[7], used by State's consular officers in issuing visas and visa revocations, the No Fly and Selectee lists used by the TSA in determining who boards flights and who gets "selected" for more thorough scrutiny,[8] and the Treasury Enforcement Communication System (TECS). Within the large communication and information system of TECS,[9] which provides critical information to 20 law enforcement agencies including the FBI, the Federal Aviation Administration (FAA) and INTERPOL, and to all points of entry into the United States, is the Interagency Border Inspection System (IBIS).

IBIS is the Department of Homeland Security's (DHS) terrorist watchlist, maintained by CBP, whose inspectors use it at air, sea, and land ports of entry, and to check incoming flight manifests from overseas to make determinations on entry and more thorough inspections at 327 ports of entry and the 15 pre-clearance offices located in Canada, the Caribbean, and Ireland. The Border Patrol uses IBIS to check on apprehended illegal crossers. The nation's state and local law enforcement also access watchlists through law enforcement data-sharing in at least three different dedicated lines, including the FBI's National Crime Information Center (NCIC).

Like TIDE, TSD contains information on both international and domestic terrorists, although the actual information on the individuals is still held separately for legal reasons. Unfortunately, those in TSD with a criminal record only include information on terrorism connectivity, and not a full history of the individual.

The 2009 Christmas Day bomber was not flagged due to gaps between TIDE and the TSD, enabling an al Qaeda recruit with a multi-year U.S. visa to board a U.S. commercial plane with a bomb sewn into his underwear. Why? Because it is the TSD, not TIDE directly, that then feeds CLASS, the No Fly and Selectee lists, and TECS/IBIS, which all have different, more rigorous requirements for inclusion as mission needs become more specific. The No Fly list is the smallest list, taking names of only about 2 percent of the TSD list; these names are only those that present an operational threat to aviation security.

Getting TIDE right, and then making good decisions about the TSD, is thus critical to the end users populating their watchlists accurately and fully. The technology that supports TIDE, TSD, and the border watchlists must work, be secure yet properly accessible, protect privacy rights, and abide by complex legal rules about how and whom to watchlist. Even so, "During FY2009 the TSC processed over 55,000 'encounters' from federal, state, local, tribal, and territorial screening agencies and entities. Of those encounters, over 19,000 were a positive match to a watchlisted known or suspected terrorist."[10] With over 22 plots disrupted on U.S. soil since 9/11, the work at the NCTC remains fundamentally important in supporting the TSC, where human analysis must work hand-in-hand with real time available data to support our national security. The "connecting the dots amongst seas of data" that characterizes watchlisting is thus crucial to how safe we are as a nation.

In short, we have made tremendous progress since the bipartisan 9/11 Commission recommendations became law in December 2004. The work that remains in part is dependent on the proper technology to embrace 9/11 (and post-9/11) policies, in part on the intelligence community prioritizing efforts against terrorist travel, and of course on the willingness of our foreign partners to continue information sharing efforts against terror that are mutually supportive. Even with a diminished al Qaeda, other state sponsor of terror threats remain, with Iran perhaps topping that list, and Hezbollah supporting cartel feuds in Mexico and infiltrating our southern border. In addition, al Qaeda's Yemeni and Iraqi factions, at minimum, still seek to abuse vulnerabilities in our border and aviation vetting to place operatives on planes and in the United States. We cannot afford complacency in watchlisting now. We know all these terrorists are actively seeking entry into the United States. We simply need to finish the task.

Key 9/11 Commission Watchlisting-Related Findings of Fact

To understand where watchlisting is today, and how far it has come, it is helpful to look back at where we were before 9/11, and recall the findings and recommendations of the 9/11 Commission that was the catalyst for so many of the intelligence community changes, including watchlisting. The core changes to watchlisting that have occurred since the publication of the 9/11 Final Report in July 2004, and the Intelligence Reform and Terrorism Prevention Act of (December) 2004 that followed from the Commission's report,[11] were due in large part to 9/11 Commission findings of fact pertaining to the failure to watchlist two known members of al Qaeda prior to 9/11. The story of the failure to watchlist began as a foreign intelligence failure and became a domestic failure in a CIA directorate called the Counterterrorism Center (CTC). The CTC was created in the mid-1980s to conduct terrorism analysis not just by the traditional regional approach used by the CIA, but a worldly approach that recognized that terrorism had no boundaries (even if falling short of recognizing the value of separate analysis on terrorist travel). In short, the story goes like this:

- The CIA knew about (1) hijackers Khalid al Mihdhar and Nawaf al Hazmi from prior investigations and an NSA intercept of a Mideast terror facility, (2) about a plane operation in Southeast Asia, and (3) travel to Kuala Lampur by both Mihdhar and Hazmi to support the plane operation in January 2000.

- The CTC briefed CIA leadership, National Security Council staff, and the FBI. However, when the CTC later learned in March 2000 from intelligence services in Bangkok that Mihdhar and Hazmi had flown into Los Angeles in mid-January, the CTC failed to tell anyone.

- The CIA put neither Mihdhar nor Hazmi on State's TIPOFF[12] watchlist. Thus, neither future hijacker could be stopped if they left the United States and tried to return, or sought another U.S. visa.

- Mihdhar did reapply for a U.S. visa in June 2001, applying for his second U.S. visa and getting it. Again, not being on a watchlist he re-entered the United States in the summer of 2001 on a brand new visa.

- Nor was Hazmi on a watchlist, and he was granted an extension of stay in July 2001.

- *Neither hijacker was watchlisted until August 24, 2001.* Without an exit-tracking system in place to determine whether the hijackers had left, the FBI trail quickly went cold and was abandoned.

Key 9/11 Commission Intelligence Community Findings of Fact

After intense scrutiny by my colleagues on the 9/11 Commission, the findings of fact regarding the multiple intelligence failures that led to 9/11 were boiled down to the following:

Problem. Too many actors with no one authority — the CIA had a separate terrorism threat center and terrorism intelligence analytic center. Numerous other agencies acted independently or cooperated on an ad hoc or limited basis with each other. These included the Defense Intelligence Agency, the DHS, and the FBI. In addition, not only were there walls preventing information sharing within, for example, the FBI and the Justice Department; higher walls existed between foreign intelligence collection (CIA) and domestic intelligence gathering (FBI).

Symptoms.

- Information was shared only on request and was highly compartmentalized.

- Dissemination remained largely internal to agencies.

- Multiple watchlists in different agencies, some classified and some not (for a total of 11 separate watchlists).

- Duplication of effort drained expertise, created redundancies, and added to a "no situational awareness" atmosphere.

Result. No one entity integrated all sources of information to see the enemy as a whole. *Because no entity saw al Qaeda as a growing threat, the U.S. government did not weigh in on the terrorist threat as it should have.*

9/11 Commission Recommendation Creating the NCTC

On page 403 of the *Final Report*, the Commission said this: "We recommend the establishment of a National Counterterrorism Center (NCTC), built on the foundation of the existing Terrorist Threat Integration Center (TTIC). This NCTC should be a center for joint operational planning and joint intelligence, staffed by personnel from various agencies." The Commission was referencing TTIC's mission. TTIC was the compliment to the CTC, providing an analysis of threats posed by terrorist organizations. Unlike the CTC, which was a CIA entity, TTIC consisted of personnel from the DHS, the FBI's Counterterrorism Division, the DCI's Counterterrorist Center, the Department of Defense, and other U.S. Government agencies. The Commission's emphasis here is across foreign and domestic intelligence collection and amongst all intelligence agencies, while consolidating action into something integrated and useful to policy making and operations. The Commission then set out the roles and responsibilities of the NCTC, and by and large, this recommendation became law later in 2004.

- "**NCTC-Intelligence** should lead strategic analysis, pooling of *all source intelligence, foreign and domestic*, about transnational terrorist organizations with global reach."

- "**NCTC-Operations** would then use threat information to create *joint operational plans*. These plans would assign operational responsibility to lead agencies" but neither direct operations nor create policy.

- "**NCTC-Authorities** would be derived from a *Presidential appointment"* confirmed by Senate with report to the Director of National Intelligence (to assure authority not undermined by sister operational entities).

9/11 Commission Recommendation on Information Sharing

While the *Final Report* provided great specificity about the NCTC's creation, the issue of information sharing transcended watchlisting, and recommendations pertaining to a watchlisting function were submerged in a discussion of information sharing that applied more broadly to all types of information used and disseminated by this community. The focus instead was on bridging the domestic/foreign divide of information within one network. Two points were emphasized:

- "The president should lead the government-wide effort… to create a *trusted information network*."
- "Intelligence gathered about transnational terrorism should be processed, turned into reports, and distributed according to the same quality standards across government, whether it is collected in Pakistan or Texas." The report goes onto say that "sources and methods should be separated from data, and all the data be classified according to the same standards — not by different standards by difference agencies — so that there is no impediment to sharing the data because of how it was obtained."

Implementation Success

After the Christmas Day Bomber, it was easy to blame the failure to keep the young Nigerian off the plane primarily on a failure to connect watchlisting dots. That was the superficial answer America was offered. The harder answer was that watchlisting had come a long way since 9/11, was vastly improved, but that a combination of fuzzy authority, inadequate communication, and incomplete analysis taken together, created a big vulnerability out of a rather small series of problems that are relatively easy to fix — at least compared to the reorganization of the intelligence community necessary after 9/11.

Thus, while issues do remain, some of them obvious and extremely important, they are not in the overall roles and responsibilities of entities as dealt with on the Commission, or in intelligence integration, but in the details of each of those issue areas, like the inability of analysts to access all data at one time. Thus, the hard part of consolidating watchlisting with one entity acting as a foundation for information (NCTC) and its affiliate (TSC) as a final adjudicator and hub of information for other agencies and partners has been solved. What remains is honing, clarifying, and upgrading until an intelligence machine that can sort and analyze vast quantities of data in real time to relevant end users is in place. The good news is we are on our way. In short, the reorganization of the intelligence community in terms of the watchlisting function can be summed up as follows:

Solved. Too many actors with no one authority:

- The DNI in charge of the intelligence community and the intelligence community is defined.[13]
- The NCTC holds the authority for intelligence integration, analysis, and dissemination.
- All watchlisting emanates from the NCTC's TIDE and is adjudicated by the TSC for the TSD.

Result. One entity (NCTC) *is integrating* all sources of information to "see the enemy as a whole;" another (TSC) *is adjudicating* final nominations, to the extent legal, privacy, and policy issues do not interfere. Thus, for the past 10 years, al Qaeda has been focused on, and today has lost significant strength in terms of an organized threat to the United States.

A Look Forward: Improving Watchlisting

The goal of watchlisting is to provide the most efficient and effective product based on the most complete information available in order to support law enforcement and intelligence goals. From my vantage point, a high priority goal is protecting the United States from nefarious entry of terrorists and their ilk. In other words, the goal of watchlisting in the border context is to significantly curtail terrorist travel.

TIDE provides our border officials with the best starting point to bear down on terrorists known to the intelligence community. The NCTC's authority to create and populate TIDE means that it is in the day-to-day activity of updating, maintaining, expanding, and culling the TIDE list that then supplies the TSD. It is the TSD's content, supplying the border and aviation watchlists, that provides the best opportunity to stop a terrorist during an immigration or aviation check. Thus, it is imperative that the process of watchlisting be done right from start to finish, every day, in both adding terrorist content and deleting entries with insufficient or inaccurate information.

While much is to be applauded in how far the intelligence community has come, the obvious failure with regard to the Christmas Day Bomber brings to mind blurry authority and processing on border referrals such as Security Advisory Opinions requested on potential terrorists in visa adjudications; incomplete information sharing; and insufficient analysis. No one seemed to be looking at the Christmas Day Bomber's travel history to the United States while weighing the bomber's father's intelligence provided to the CIA officer at the U.S. Embassy in Nigeria to help determine the credibility of his story. The CIA officer was not talking to embassy staff to get visa history and relating that back to the NCTC to insure his analysis of the bomber's father's information was accurate. The list goes on. These problems are ones of incomplete analysis, un-delineated responsibilities, and failures by DHS in creating traveler histories (a 9/11 Commission recommendation) to support the intelligence and border law enforcement communities to determine potential terrorist linkages. These problems also highlight the importance of biometrics more generally, for more accurate identification of a suspect and again, potential terror linkages.

So where does watchlisting need to go from here?

Complete Information Access for Analysts. In the vast sea of information where literally hundreds of names a day are barraging analysts for potential inclusion in the TIDE watchlist, it is essential that technology and software support processing seamlessly, assuring that those who need data get what they need without multiple searches across multiple data sets. As I understand it, there remains an issue with those in need-to-know areas still not getting sufficient access to classified data, especially in the area of foreign versus domestic collection. While not privy to the reasons or details for this, I am assured this is a serious issue discussed by the 9/11 Commission and not sufficiently solved at this time. Because the issue is a classified one, it is up to congressional committees with intelligence community oversight to work with the NCTC on fixing the gaps, and vetting vendors who can help bridge those gaps, solving any legal issues as they move forward.

This is where the availability of appropriate technology comes into play. Content need not be less available simply over issues of security and privacy. Technology is available today to assure that silos of information and classification can be tagged to be cross-searched to make data access and exchange fast and efficient; ensure privacy up and down silos of information; are encrypted and protected indefinitely throughout time; and that "keys" to information are held per silo, so even the breach of one silo does not mean a successful hack into an entire database, as we have seen time and again recently.

In addition, "cloud computing"[14] is a service-oriented architecture that allows data to be pulled based on rules and available to intelligence and law enforcement customers on an "as needed" basis. For example, TSA alone has about 15 systems to collect information on those seeking access to secure areas in the sea, air, and land transportation modes. The best known of these is the Transportation Workers Identification Card (TWIC), but others exist for those seeking hazardous materials licenses and qualifying as aviation workers, for example. None of these data sets are available system-wide or talk to each other, creating inefficiencies. Failure to easily access this data also denies NCTC and TSC analysts potential critical information to make better watchlist decisions or determine trends in terrorist travel or embedding tactics here in the United States. With cloud computing, all this data would be retained remotely and be stored in the same area, yet protected by dynamic encryption keys that change with new users and siphon information based on "tagging" similar to that used in the internet environment and the "rules" traditionally used by the intelligence community to help define and prioritize vast amounts of incoming data.

Such technology helps solve multiple issues: (1) connecting the dots in a sea of information; (2) enabling agencies to share critical information to ensure our screening systems catch known terrorists; (3) assuring that the right people at the right time get the right information; (4) protecting data from hacking or corruption while simultaneously transferring "keys" to access information; (5) doubling down on creating and maintaining the best information and the right identities — and only the right identities — on rigorous watchlists, like TSA's No-Fly and Selectee lists; (6) enabling better trend analysis of terrorist travel and embedding tactics; and (7) enabling a quantifiable larger amount of data to be dealt with on a long term basis, minimizing concerns about overloaded systems.

Full Biometrics. TIDE vetting must move forward in a manageable, scalable, and useful way. The best way to accommodate public squabbles over inaccuracy of the list and misidentifications, and let analysts focus on true terrorist identities, is to build biometrics into TIDE vetting and data. Those biometrics can be useful to customers on an as-needed basis. HSPD-24 requires the FBI's Criminal Justice Information Services Division to work with the NCTC to be able to hold, receive, and export terrorist data pertaining to biometrics.[15]

Such biometrics include, for example, domestic facial recognition digital images from state Motor Vehicle Departments disseminated for law enforcement purposes. Other types of biometrics include those from state criminal databases and fingerprints lifted from foreign terrorist crime scenes, safe houses, and bombs and those acquired from international partners. Since

2004, US-VISIT[16] captures 10 prints at ports of entry and takes and compares digital images of foreigners at ports of entry, working hand-in-hand with the FBI's IAFIS[17] rolled 10-print database. US-VISIT significantly reduces passport fraud by aliens, including terrorists and criminals. US-VISIT also biometrically assures that derogatory information on an individual is not a false positive, and removal or apprehension of the individual is based on accurate information.

These are only a handful of common scenarios where biometrics are vital to better assuring border security. Just recently, we were reminded again of the critical need to tap into biometrics when adjudicating travelers. In this case Iraqi refugees (whose status is permanent in the United States) were not fully vetted by an Army biometric database of prints found and analyzed forensically by the FBI on defused Iraqi bombs.[18] An entire population of Iraqi refugees was admitted without this check. Why was this inexcusable? The intelligence community later learned, after 58,000 Iraqi refugees were processed, that al Qaeda in Iraq and Yemen were seeking to exploit this same refugee process for entry by their operatives. This is Terrorist Travel 101: Terrorists will exploit whatever border vulnerabilities exist to get in and stay in the United States. The refugee process has always been vulnerable, as it is difficult in the field for adjudicators to determine veracity among such populations. Biometrics go a long way in determining if an individual has terrorist ties, no matter what they tell an immigration adjudicator. A *Los Angeles Times* story describes the issue with one such terrorist missed in this population:

> "In the Kentucky case, the FBI learned in November from a confidential informant that Waad Ramadan Alwan had constructed improvised roadside bombs in Iraq before he was granted U.S. asylum in April 2009.
>
> "Alwan allegedly told the informant that he had planted bombs near the oil refinery town of Baiji in northern Iraq in summer 2005. In December, the FBI's field office in Louisville asked for help from the FBI-run Terrorist Explosive Device Analytical Center in Quantico, Va.
>
> "The little-known center warehouses more than 70,000 defused bombs, all recovered in Iraq and Afghanistan since 2003, for possible use as evidence. The stockpile is so large that 300 forensics experts and other technicians are assigned to respond to requests from investigators or intelligence analysts.
>
> "In January, after checking several thousand items in the inventory, the FBI said it had found Alwan's fingerprints on a cordless phone that had been wired to detonate an improvised bomb near Baiji in 2005.
>
> "A bomb squad had found the phone and sent it to Quantico. But it was labeled 'low priority' and was not dusted for fingerprints until this year, said a U.S. law enforcement official who requested anonymity to discuss an ongoing investigation."

As a result of failure to run prints on the Iraqi refugee population, brought to light further by this Kentucky case, 300 of 58,000 Iraqi refugee applications are currently being re-vetted through the Army database at a potentially significant cost to our national security. This oversight happened for two reasons, apparently: (1) the Army is concerned about hacking into a sensitive biometric database; and (2) even without this concern, the FBI was years behind in forensically lifting the prints, processing them, and making them available to the Army database. When biometrics are not used upfront in the vetting process, legitimate travelers and immigrants can get caught in the crosshairs while terrorists can slip through by abusing the vulnerabilities of a name-based system. There is no excuse for that mistake in today's technology market, where solutions exist for protecting, while also properly disseminating, sensitive data.

Another example of how biometrics applies to national security issues is a scenario borne out of the Southwest border crisis, where Hezbollah tattoos are appearing on apprehended Mexican drug cartel members. Latent prints of foreign nationals with a U.S. criminal history, or prior entry into the United States, are available to the Border Patrol through IAFIS/IDENT.[19] If a print previously has been picked up from an underground drug stash house on the U.S. side of the border and linked to a tunnel built with support from Hezbollah, for example, then it may just be that print that helps identify this individual further with both a particular cartel *and* Hezbollah, making an otherwise removable individual require further investigation. The intelligence gleaned by making a positive identification on a known or suspected drug cartel/terrorist operative could potentially unravel a host of alien, drug, and potential terrorist activities otherwise unknown.

The law enforcement and intelligence value of establishing the identity of a Hezbollah-connected Mexican drug cartel member is clear. Yet there is another benefit to accurate biometric identification of an otherwise anonymous entry: establishing identity in this circumstance puts fear into cartel members and terrorists that the anonymity they rely on when illegally crossing our borders is no longer possible. The resulting scenario instead could be uncomfortably shown to be similar to al Qaeda after 9/11: the United States can identify your operatives even if they were initially anonymous, and this time not because of airline manifest lists and phone calls from passengers and astute flight attendants, but because of biometrics consistently applied to those who present a possible security breach for our country. Biometrics are the data you always carry on you, and cannot change. This is not good news for a terrorist who wants to avoid detection.

Full Incorporation of Traveler and Visa Security Unit Information from All Immigration Agency Sources into Watchlist Vetting. Streamlining the divide between immigration agencies and foreign persons should have been completed by now with consolidated, person-centric "traveler histories." This is a core 9/11 Commission recommendation I particularly insisted on among my colleagues on the Commission staff. Prior to 9/11, fraud was perpetrated throughout the system by those simply trying to stay here legally as well as criminals and terrorists. One common fraud technique was for the same person to change names and apply for immigration benefits in multiple regions just to try to get through the system successfully and more quickly. It was relatively easy to game the system for whatever immigration benefits were sought in the absence of traveler histories incorporating information on visa issuance, entries, exits, security and criminal information, biometrics, immigration benefits and overstays, pending removals and deportations, returning without a legal basis to enter, or seeking immigration benefits without a legal basis to access those benefits.

There are still no comprehensive traveler histories that bridge the information divide between State, CBP, Immigration and Customs Enforcement (ICE), and U.S. Citizenship and Immigration Services (USCIS), providing a single set of data described above, including relevant biometrics and law enforcement or intelligence data. This is a missed opportunity to create, automatically, terrorist travel dossiers that could provide a vast amount of operational and analytic data to the NCTC and other entities charged with determining who is on and off watchlists. This is a serious flaw that also denies critical information to border officials. "Personcentric" traveler histories could highlight a nexus to terror or fraud whenever a terrorist encounters an immigration or law enforcement entity. There is no excuse, at this point, for such data not being compiled automatically for NCTC analysts, and others in the intelligence community. It would ease the NCTC and TSC's burden significantly, but it is up to DHS to fulfill this legal requirement.

That being said, there is a relatively new source of information useful to TIDE vetting from ICE Visa Security Units (VSUs) at 19 U.S. embassies (with more expected) that has emerged since 9/11 that intelligence analysts should take seriously. The fact still remains that foreign terrorist organizations that seek to do us harm are in fact often recruited from a foreign population. (Only about 2 percent of the Terrorist Watchlist consists of U.S. citizens or legal permanent residents.) This means that reliable data obtained by American law enforcement abroad, which is tailored to what our intelligence and law enforcement communities need, supplies critical information on the TIDE population.

ICE's Visa Security Officers conducting cases from abroad, alongside consular officers and diplomatic security officers from State, provide not only essential identity information in the visa process, but also investigative material on potential terrorists, linkages to organizations and other terrorists, counterfeit and fraud techniques, and operational information. Such information should be treated as having solid weight with the intelligence community.

Currently, the House Judiciary Committee seeks to give DHS control of not only visa policy, but visa revocations as well. If that proposal became law, the VSUs' stature and ability to control their caseload would become more firmly rooted as a consistently growing source of material for intelligence analysis (assuming Congress funds this program). In addition, if the standard for visa revocation is fully oriented around national security, the work of the NCTC should align even more closely with visa adjudication and revocation, helping TIDE do a better job of making recommendations to the TSD as well as support Security Advisory Opinions on visa issuance. In turn, such improvements in data should be incorporated into the CLASS watchlist State uses in visa adjudication and the IBIS database ICE uses in VSU reviews, bringing the work on counter terrorist travel full circle, and well honed. See the Appendix on p. 14 for recent testimony.

Passenger Name Record Data. While TIDE and the TSC work to provide quality control over the thousands of names populating its list, when it comes to air and sea travel to the United States, it is the Passenger Name Records (PNR) that provides the vital data run against existing data in the TSC's Terrorist Watchlist. PNR identification data includes full name, gender, date of birth, passport information, and full itinerary of a traveler that have already been shared with at least the air or sea carrier, and possibly a travel agency, car rental agency, or lodging as well. Airlines use the information to analyze trends in travel routes and demographics to better hone marketing. The United States uses PNR data to electronically check for terrorists, using the more extensive PNR data to assure that a positive watchlist match is indeed a match, and not a false positive. PNR data are also used to make sure that those who pose a threat to national security are not permitted in the country while those who are a potential threat to aviation security found to match a "No Fly" or "Selectee" name when run through the TSA Secure Flight interface,[20] are not allowed to fly, or are at least screened more thoroughly.

Procedurally, the PNR data support the watchlisting function as follows: prior to being issued a boarding pass, a customer will have had his PNR data run against TSA's subset of the Terrorist Watchlist held in the Secure Flight system, checking against the "No Fly" and "Selectee" databases. If there is no match, a boarding pass is issued. If there is an initial positive match, a TSA analyst residing at the TSC will search again the TIDE database to eliminate any false positives or better determine that no boarding pass should be issued. If the passenger is foreign, then actually receiving the PNR data takes front and center in terms of importance; without the data, our watchlists have little to check against but manifest lists from airlines once in the air. That presents a Christmas Day Bomber scenario once again.

Why discuss this issue? If too many limitations are put on the type, use, and legalities of use of that data, as the European Union is currently attempting to do — despite signing a seven-year agreement on its use in 2007 — then TSA/TSC will be extremely limited in doing its job, and the United States will have a diminished ability to secure against terrorist travel *and* aviation threats.

Support an Electronic System for Travelers (ESTA) Approach for Multi-Entry Visa Holders. ESTA currently requires that visa waiver travelers, prior to U.S. travel, fill out online pre-travel forms that check against watchlists. Approval with ESTA lasts two years, in essence acting as a mini-visa. "Visa waiver" travelers reside in countries whose citizens do not need U.S. visas for 90 day visits; they need only apply for entry at the U.S. border.[21] Visa waiver countries enter into bilateral agreements with the United States and have met certain criteria to enter the program, such as low immigration rates to the United States; their citizens do not tend to overstay their visas; and that government is willing to provide watchlist and criminal information on their populations to ensure that criminals and terrorists do not enter the United States. The visa waiver currently covers most of Europe. Thus, it is their citizens seeking to travel to the United States who are checked in real time for derogatory information that may have accrued only 24 hours prior via ESTA. If a traveler has filled out an ESTA within the previous two years, it is at this point PNR data is relied on at the time of travel to determine if any new derogatory information has accrued.[22]

Ironically, ESTA vetting does not occur for all the other countries in the world that are not in the visa waiver program, including those known to host anti-American terrorist populations. Once a visa is issued, often for multiple entries and up to five years in duration, derogatory information is not routinely checked again prior to travel. Only PNR data is, and that is not done until issuance of the boarding pass. Thus, the Christmas Day Bomber was easily able to board a plane without any potential additional screening until immediately prior to arrival here in the United States, because in 2009, PNR was only vetted in-flight. Today, the Christmas Day Bomber would be screened via PNR data before boarding, but not when the reservations were made, as ESTA does. Keeping the Christmas Day Bomber out of the airport, and requiring him to return to the embassy for a visa review, might have scared off al Qaeda enough not to even attempt the bombing.

Our current policy of failing to quietly re-screen visa holders immediately prior to travel makes no sense from a national security perspective; rather, it is essential that all travelers be vetted for any newly developed derogatory information. There is no excuse that travelers from the generally friendly nations covered by visa waiver are vetted against watchlists before travel every two years while those from other countries, including many that are not our friends, are not receiving such vetting until they arrive at the airport. It makes little sense that the British and Germans have to receive an ESTA vetting at time of reservation, for example, while those from Yemen, Somalia, and Pakistan do not.

If there appears to be a potential harm to aviation due to information gathered and knowledge of such air reservations booked to the United States, a priority should be set to vet thoroughly and quickly. Today, no such standards are in place. Since there are no requirements now for consular officers to run names through

CLASS before travel, it is imperative that the NCTC realize this and *not* rely on State to initiate inquiries, if possible. Nor does it make sense to allow our foreign partners, especially in the European Union, that agreed to provide us the key traveler information necessary to keep terrorists off of U.S.-bound planes, to renege on those agreements now.

Recently, in response to the Christmas Day Bomber, the intelligence community was criticized by Congress for attempting to create a risk-assessment program to profile travelers entering and leaving the United States. Congressional disapproval was justified. Profiling is unnecessary and inefficient. Instead, an ESTA-style automatic watchlist vetting system, defined amongst State, DHS, and the intelligence community, with TSA's inclusion, applicable to all those traveling to the United States with few exceptions, would provide a solid means to shore up overseas pre-travel vetting to keep terrorists off of planes, whether it is just for travel or to commit an operation on the plane. The result would be that no terrorist, or his sponsoring organization or nation, would feel comfortable that he can safely travel simply because a U.S. visa was obtained a few years earlier.

Recommendations

The 10 years since 9/11 have dramatically changed the roles and responsibilities of watchlisting, and watchlisting itself, for the better.

- Huge strides have been made in developing watchlisting protocols that meet relevant legislative and Presidential Directives for a generic Terrorist Watchlist that supports a variety of intelligence and law enforcement customers both in and out of the United States. Aggregating that data and cleanly delineating that the right customers are receiving the right data in a secure manner requires upgrades to technology that are not currently incorporated into the everyday information-sharing environment at the NCTC and TSC. Cloud computing and dynamic encryption technologies are available, and need to be incorporated into the daily life of the NCTC and TSC as soon as possible. Though time-consuming, it is a necessary and worthwhile effort.

- Preventing terrorist travel requires the NCTC and the TSC to prioritize the incorporation of "person-centric" traveler information, including the information produced by VSUs, into terrorist dossiers that are available to the intelligence community for watchlisting purposes as well as to State, CBP, ICE, and USCIS analysts assigned to review information on incoming travelers or on those already in the United States seeking immigration benefits. Providing such person-centric traveler histories is a requirement borne by DHS, which to date has not been fulfilled. This will also allow foreign persons applying for benefits to have their information held over time, minimizing fraud on the one hand while easing processing of new benefits sought, because information will not need to be re-populated, as caching now does for websites. Where privacy issues exist, these can be written into the information-sharing rules up front.

- Name-based information is always more solid when combined with biometrics to better assure identity. TIDE should work to include a biometric in every terrorist dossier as soon as possible. Doing so will hone the Terrorist Watchlist, and its border watchlist subsets, so they are accurate and do not misidentify legitimate travelers, and do not miss terrorists.

- Law enforcement data obtained from abroad by Immigration and Custom Enforcement Visa Security Units conducting terrorist investigations of visa applicants abroad need to be incorporated into watchlist analysis. Congress needs to prioritize the VSU expansion, and give DHS visa revocation authority. The United States must do what it can to keep European Union agreements in place pertaining to Passenger Name Records; these records are absolutely essential to assuring accuracy of matching watchlist information to relevant aviation travelers.

- All visa holders and visa waiver participants should have their information vetted at least every two years, and every time they seek to travel to the United States. Protocols need to be in place for non-visa waiver travelers; an expansion of ESTA to all valid visas older than two years would even out the vetting protocol so that citizens from non-visa waiver nations, including state sponsors or state harborers of terror, would receive the same vetting as travelers from friendly visa-waiver countries. The current state of vetting on travelers is a tad perverse, and requires some common-sense adjusting. Applying a standardized approach avoids profiling, establishes security away from our borders, and enables real-time vetting where derogatory information develops after visa issuance. Eventually, with cloud technology, vetting could be done in real time, on a daily basis if necessary, for all visa holders.

End Notes

[1] http://www.nctc.gov/docs/Tide_Fact_Sheet.pdf. Traditionally only the FBI populated "U.S. persons" onto watchlists. "U.S. persons" are (1) U.S. citizens or legal permanent residents or (2) a U.S. corporation and (3) not under direction from a foreign terrorist organization or state.

[2] Testimony of Timothy Healy, Terrorist Screening Center Director, Federal Bureau of Investigation, before Senate Homeland Security and Governmental Affairs Committee, December 9, 2009, Hearing on Five Years after the Intelligence Reform & Terrorism Act: Stopping Terrorist Travel, at http://hsgac.senate.gov/public/index.cfm?FuseAction=Files.View&FileStore_id=50242372-f66d-401f-b3a8-1feb2b2de-6fa.

[3] *Ibid.*

[4] http://narcosphere.narconews.com/userfiles/70/ice_memo.pdf.

[5] 9/11 Commission *Final Report*, p. 403-406.

[6] For HSPD-6 full text, see http://www.dhs.gov/xabout/laws/gc_1214594853475.shtm.

[7] For a lengthy discussion of CLASS and its upgrades since 9/11, see Testimony of Janice L. Jacobs, Assistant Secretary of State for Consular Affairs before the Senate Committee on Homeland Security & Governmental Affairs, December 9, 2009, Hearing on Five Years after the Intelligence Reform & Terrorism Act: Stopping Terrorist Travel , at http://travel.state.gov/law/legal/testimony/testimony_4612.html.

[8] For the most recent DHS in-depth discussion of the rollout of Secure Flight, the system providing access to the No Fly and Selectee lists, see http://www.tsa.gov/press/releases/2008/1022.shtm.

[9] For more on the exact content of TECS, and with what entities it provides data, see http://cryptome.info/irs-ci/36426.html#ss1.

[10] Testimony of Timothy Healy, Terrorist Screening Center Director, Federal Bureau of Investigation, before Senate Homeland Security and Governmental Affairs Committee, December 9, 2009, Hearing on Five Years after the Intelligence Reform & Terrorism Act: Stopping Terrorist Travel, at http://hsgac.senate.gov/public/index.cfm?FuseAction=Files.View&FileStore_id=50242372-f66d-401f-b3a8-1feb2b2de-6fa.

[11] Conference Report for the Intelligence Reform and Terrorism Prevention Act of 2004, http://www.gpoaccess.gov/serialset/creports/intel_reform.html.

[12] TIPOFF was State Department's watchlist and the predecessor of TIDE; the one watchlist of the pre-9/11 11 lists chosen to provide the foundation for the current Terrorist Watchlist.

[13] However, authority needs to be more clearly delineated in gray areas, such as security opinions on immigration-related matters, (as was the case with the Christmas Day Bomber; these issues are still not resolved), that often are not addressed until something happens to highlight what has gone wrong.

[14] For an explanation of cloud computing, see Jonathan Strickland, "How Cloud Computing Works", http://computer.howstuffworks.com/cloud-computing/cloud-computing.htm.

[15] For the full text of Homeland Security Presidential Directive 24: Biometrics for Identification and Screening to Enhance National Security, see http://www.dhs.gov/xabout/laws/gc_1219257118875.shtm.

[16] For more on US VISIT, see http://www.dhs.gov/files/programs/usv.shtm.

[17] For more on IAFIS, see http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis.

[18] Brian Bennett, the *Los Angeles Times*, "Iraqi refugees in U.S. rechecked for terrorism links: Officials fear lapses in immigration security may have let insurgents and potential terrorists enter the country. More than 58,000 Iraqis are being screened again", July 18, 2011, http://articles.latimes.com/2011/jul/18/nation/la-na-refugee-terror-20110719.

[19] For the integration of IDENT and IAFIS in 2001, see www.justice.gov/oig/reports/plus/e0203/back.htm; for full operational access to 10 prints, see http://www.visalaw.com/print/12sep404.html; for DHS immigration community holding largest biometric database in the world with over 89 million fingerprint scans, see http://eagle2.bstonetech.com/node/47.

[20] Secure Flight became fully implemented with all air carriers flying to the United States and within the United States in 2010 after prior systems, begun in the late 1990s, failed for a variety of reasons. Its main purpose is to take the watchlisting check away from air carriers and make the No Fly and Selectee checks a government function, to standardize use, better maintain confidentiality of the list, and prevent misidentification of travelers by incorporating gender and date of birth. For more on Secure Flight, see TSA's Fact Sheet at http://www.tsa.gov/what_we_do/layers/secureflight/faqs.shtm.

[21] See http://travel.state.gov/visa/temp/without/without_1990.html.

[22] For how the PNR data works, and its value to the intelligence community, see http://hosteddocs.ittoolbox.com/AK052307.pdf.

Appendix

On May 11, 2011, I testified before the House Judiciary Subcommittee on Immigration Policy and Enforcement on "Visa Security: Preventing Terrorists from Abusing U.S. Immigration Policy." This oral testimony discusses both the VSUs and Electronic System for Travelers (ESTA), and provides background on why the two are essential for securing our borders. The relevant portions are as follows:

The 9/11 Commission recommendations emphasize that terrorists are best stopped when "they move through defined channels." Remember that of 23 hijacker applications, 22 were approved.

The first, and best, opportunity to stop terrorist travel is in the visa adjudication process, where triggers for further investigation can mimic what should have been triggers for the 9/11 hijackers such as recently obtained new passports; suspicious or fraudulent travel stamps; indicators of extremism; or incomplete or fraudulent applications; or, easiest of all, watchlisting by the intelligence community.

However, new terrorist travel methods constantly evolve, and it is DHS and Immigration and Customs Enforcement that have the best access to the information and expertise to expose those methods because it is ICE that holds open case information and sensitive information on terrorists cases abroad, not the State Department whose consular officers adjudicate the visas today. In addition- ***and this is really important to the discussion today —*** *a foreign national's affiliation with terrorism may develop after —* ***or because of*** *— an already existing U.S. visa.*

Osama bin Laden and Khalid Sheikh Muhammad specifically sought out individuals with existing U.S. visas. Thus, in my view, visas need periodic review, especially prior to U.S. —bound travel. Revocation investigations need to be as robust as those conducted by Visa Security Units prior to visa issuance. In fact, visa revocations can be a linchpin to deny entry, or support removal of those already in the United States.

With the death of Bin Laden, and an increase in retaliatory statements by Al Qaeda, we may now experience even more splintering of Al Qaeda into factions or lone wolf-type terrorists. Our consular posts will be under more pressure than ever to get visa adjudications right, most particularly in ***visa-issuing countries where currently there is no formal policy on pre-travel vetting****. Today, visa waiver travelers coming for business or pleasure are vetted through ESTA, a DHS travel authorization program which operates as a virtual, mini-visa for nationals of visa waiver countries. But visa issuing countries have no such standardized pre-travel vetting. This is a significant gap. VSUs should be doing pre-travel vetting of visas in visa issuing countries in order to provide a stop gap before the time pressures of US-bound international flights. In these instances, revocations could occur without the threat posed by pending airline travel of a terrorist such as the Christmas Day bomber.*

From the lens of a former 9/11 Commission staffer, my view is that extending visa revocation authority to DHS and expanding VSUs worldwide is common sense from a legal, policy, and bureaucratic view point. VSP security related reviews in high risk areas of the world and throughout the visa process are essential. From a policy perspective, security must trump infrastructure, political or diplomatic considerations that are not always in line with security decisions.

From a legal perspective, it is DHS that is responsible for both homeland security and border security. Thus, what VSUs add to security of visa processing at consulates overseas is invaluable, because that is what they do. The State Department lists its top mission as diplomacy, as it should be. Diplomacy is a vital and necessary function, but 'border security' is never mentioned in this administration's State Department mission statement. Thus, State's Chief of Missions should not have a say in determining VSU presence at a consular post.

Moreover, expanding VSP authority to national security related revocations is feasible. The VSUs combine intelligence, operations, and law enforcement to intercept terrorists and constrain terrorist mobility by recommending refusal of visas, creating lookouts in government databases, conducting secondary interviews of applicants, identifying terrorist travel trends and tactics, and nominating watchlist candidates. In just eight posts two years ago, ICE special agents had recommended 750 visas be denied, created 933 lookouts, and dealt with over 100 potential terrorists. Very little of this activity would happen but for the VSP.

Our national security depends, in part, on the robustness of our border security to keep out foreign nationals with nefarious intentions -- and keep them as far away from the United States as possible. Counterterrorism efforts outside of our physical borders and throughout the entire visa process in ***both*** *issuance and revocation—must be as secure as possible. The entity with the mission, expertise and bureaucratic functioning on national security related immigration cases is DHS. In addition, DHS already has visa authority by law in issuance, and an extension of that authority to revocations makes sense.*

* *http://cis.org/node/2784.*

Backgrounder

Border Watchlisting a Decade after 9/11

By Janice Kephart

The tedious process of watchlisting and making watchlists available to our frontline border and aviation operators is the most important tool our nation has to curtail attempted "legitimate" terrorist travel — meaning, those terrorists who seek to use our border and aviation system to enter the United States. The 9/11 Commission recommended significant changes to watchlisting, including merging 11 disparate watchlists into one base list. Today, this single list is simply termed the "Terrorist Watchlist." The entity recommended to accomplish this goal was, and now is, the National Counterterrorism Center (NCTC). The Commission's focus on watchlisting addresses — in part — findings of fact of missed watchlist opportunities of (at least) two 9/11 hijackers who were known to the CIA in March 2000, but whose entry into the United States was never communicated to the border, aviation, or other members of the intelligence community until August 24, 2001.

Center for Immigration Studies
1522 K Street, NW, Suite 820
Washington, DC 20005-1202
(202) 466-8185 • (202) 466-8076
center@cis.org • www.cis.org

Support the Center through the Combined Federal Campaign by designating **10298** on the campaign pledge card.

Center for Immigration Studies
1522 K Street, NW, Suite 820
Washington, DC 20005-1202
(202) 466-8185
center@cis.org
www.cis.org