S. HRG. 111–616

SECURING AMERICA'S SAFETY: IMPROVING THE EFFECTIVENESS OF ANTITERRORISM TOOLS AND INTERAGENCY COMMUNICATION

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED ELEVENTH CONGRESS

SECOND SESSION

JANUARY 20, 2010

Serial No. J–111–71

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE

58–484 PDF WASHINGTON : 2010

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

QUESTIONS AND ANSWERS

Question#:	1
Topic:	privacy guidelines
Hearing:	Securing America's Safety: Improving the Effectiveness of Anti - Terrorism Tools and Inter-Agency Communication
Primary:	The Honorable Russell D. Feingold
Committee:	JUDICIARY (SENATE)

Question: According to the TSA website, TSA has established privacy guidelines for the use of imaging technology at airports, including that the agent viewing the images is not at the checkpoint; the agent at the checkpoint never sees the image; the faces in the images are automatically blurred; and the images are not stored or shared.

Is TSA considering enshrining these rules in formal regulations?

What enforcement mechanisms are currently in place to ensure that these privacy protections are being followed?

What privacy restrictions apply if the screening is being conducted by a foreign entity?

Response: The Transportation Security Administration (TSA) is committed to preserving privacy in its security programs and believes strongly that the Advanced Imaging Technology (AIT) program accomplishes that through a screening protocol that ensures anonymity for the individual undergoing the AIT scan. This is achieved by physically separating the Transportation Security Officer viewing the image from the person undergoing the scan. This officer sits in a windowless room that is separated from the checkpoint. The AIT scans cannot be printed, stored or retained in an operational setting, and the operator cannot change the storage or retention features of the unit. Cameras and cell phones are not allowed in the viewing room under any circumstances. The images produced by both backscatter and millimeter wave technology do not identify a specific individual. Further anonymity protection is achieved in the millimeter wave technology by a filter on the scanned image that blurs the face of the individual who was scanned. Finally, if a passenger is still concerned about privacy and does not want to undergo AIT screening, they can opt for alternative screening.

The privacy guidelines are included in TSA's Privacy Impact Assessment (PIA) for AIT first published in January 2008 prior to the use of the devices in the AIT pilot. The PIA and standard operating procedures govern the operation of AIT. Enforcement of the guidelines is achieved through acceptance testing of each device at the manufacturer and at installation, and through operator training and supervision in the airport setting both at the screening checkpoint and the image viewing room.

Privacy restrictions in foreign settings are established by each individual nation and vary widely from no restrictions to protocols consistent with those used by TSA. TSA is unaware of any entity using greater privacy protocols than TSA.

Question#:	2
Topic:	ETP
Hearing:	Securing America's Safety: Improving the Effectiveness of Anti - Terrorism Tools and Inter-Agency Communication
Primary:	The Honorable Russell D. Feingold
Committee:	JUDICIARY (SENATE)

Question: Explosive Trace Portal (ETP) technology is designed to detect the types of explosives that Abdulmutallab was carrying on Christmas Day. However, according to an October 2009 GAO report, ETP technology was deployed in airports before it was adequately tested and had substantial performance problems.

Is DHS still considering the use of ETP or any other explosives detection technology?

What resources, if any, are being devoted to research and development of an improved version of ETP or other explosives detection technology?

Has any analysis been conducted on the relative efficacy and costs of ETP versus body imaging technology?

Response: As of December 31, 2009, nine Explosive Trace Portals (ETP) were in use. While the ETP devices previously purchased by the Transportation Security Administration (TSA) experienced operational performance issues that hindered their effectiveness in the field, TSA and the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) continue to evaluate a variety of trace detection technologies. TSA estimates that the two currently deployed ETPs will be replaced by the end of calendar year 2010 as TSA continues its aggressive deployments of Advanced Imaging Technology (AIT). DHS S&T continues to perform research on a variety of trace detection technologies, including both portable and tabletop explosive trace detectors and shoe scanning devices. Results of this research will be utilized by TSA to plan for new security technology projects or for the addition of new functionality to existing devices within the checkpoint. No specific comparison studies of the efficacy and costs of ETP versus body imaging technology have been conducted. Body imaging technology provides TSA with an entirely different detection technology from explosive trace portal equipment. ETP collects and analyzes the surrounding air for traces of explosive particles, while body imaging technology presents an image of the passenger and of all items on a passenger's body to detect prohibited items.

Question#:	3
Topic:	GAO
Hearing:	Securing America's Safety: Improving the Effectiveness of Anti - Terrorism Tools and Inter-Agency Communication
Primary:	The Honorable Russell D. Feingold
Committee:	JUDICIARY (SENATE)

Question: An October 2009 GAO report indicates that TSA officials planned to develop a cost-benefit analysis of various passenger screening technologies, but that time frames for such an analysis could not be provided. Has a time frame for this analysis been established since that report, and if so what is it?

Response: In evaluating and procuring new technologies, the Transportation Security Administration (TSA) continues to use a structured methodology and process that complies with requirements specified by the Department of Homeland Security (DHS) Acquisitions Directive (AD) 102. As a requirement of DHS AD102, projects must generate Life Cycle Cost Estimates (LCCEs) based on known and estimated costs, which are presented at prescribed instances, or Acquisition Decision Events (ADEs). These LCCEs will be combined with the results of Risk Management Analysis Process (RMAP) case studies (currently in process) which detail the threat reduction of deployed technologies. In addition, yearly TSA Investment Review Boards and DHS Acquisition Review Boards review the PSP program as a portfolio of technology projects to include information regarding both costs and benefits (e.g. reduction of risk).

Acquisition Review Boards at TSA and DHS are scheduled at various times as projects enter an acquisition phase requiring milestone decisions to proceed.

Question#:	4
Topic:	resources
Hearing:	Securing America's Safety: Improving the Effectiveness of Anti - Terrorism Tools and Inter-Agency Communication
Primary:	The Honorable Russell D. Feingold
Committee:	JUDICIARY (SENATE)

Question: Has DHS or TSA done any analysis of the effect on TSA and the need for additional resources if the number of people who were treated as selectees were to increase dramatically?

Response: Our analysis of all Terrorist Identities Datamart Environment (TIDE) records indicates minimal impact to our checkpoint operation. However, increasing the number of people treated as selectees could have an impact on the vetting and redress operations for aviation passengers and those individuals required to undergo a Transportation Security Administration administered Security Threat Assessment prior to the issuance of a credential or benefit in all modes of transportation.

Question#:	5
Topic:	alternatives
Hearing:	Securing America's Safety: Improving the Effectiveness of Anti - Terrorism Tools and Inter-Agency Communication
Primary:	The Honorable Russell D. Feingold
Committee:	JUDICIARY (SENATE)

Question: Has DHS considered alternatives to the policy of requiring all nationals from 14 countries, as well as anyone traveling from or through those countries, to go through enhanced screening? If so, what alternatives have been considered? Have they been rejected, and if so why?

Response: The Transportation Security Administration (TSA) has implemented enhanced security measures for all international flights to the United States. The decision to list any country as a "country of interest" does not depend on any single event or piece of information. The inclusion of a country reflects a careful assessment of various factors, to include those states considered to be safe havens for terrorists and those that are State sponsors of terrorism, as assessed by the Department of State in its Country Reports on Terrorism, as well as current information provided by the Intelligence Community.

TSA and the interagency community (including the Department of State) regularly reviews and modifies the list as circumstances and the assessment of the risk of attacks warrant. In order to identify mitigation options to counter new and emerging threats to aviation, including the threat posed by the December 25, 2009, incident, TSA continues to work closely with its international partners and participates in several international outreach events.

Question#:	6
Topic:	security
Hearing:	Securing America's Safety: Improving the Effectiveness of Anti - Terrorism Tools and Inter-Agency Communication
Primary:	The Honorable Dianne Feinstein
Committee:	JUDICIARY (SENATE)

Question: According to the Department of Homeland Security, the Transportation Security Administration (TSA) has implemented 20 layers of security at our nation's airports. The airport security checkpoints, however, constitute only one security layer of the many in place to protect aviation. Others include intelligence gathering and analysis, checking passenger manifests against watch lists, random canine team searches at airports, federal air marshals, federal flight deck officers and more security measures both visible and invisible to the public.

Can you describe what additional efforts DHS is undertaking to improve airport security and how DHS is measuring the effectiveness of deploying full body scanners at airport security checkpoints?

Response: In addition to the security layers mentioned above – airport security checkpoints, intelligence gathering, watch lists, canine teams, Federal Air Marshals and Federal Flight Deck Officers – the Department of Homeland Security (DHS) is actively working on a number of initiatives to improve security at our Nation's airports. DHS is working with our interagency partners in evaluating the process by which names are added to the No-Fly and Selectee Lists to determine if adjustments are appropriate. DHS is primarily a consumer of the terrorist watch list, and we are working closely with our partners in the Intelligence Community to make clear the kind of information DHS needs from the watch list system. DHS is establishing a partnership on aviation security with the Department of Energy and its National Laboratories to use its expertise to bolster our security by developing new and more effective technologies that deter and disrupt known threats and anticipate and protect against new ways that terrorists could seek to board an aircraft with dangerous materials. DHS is accelerating deployment of Advanced Imaging Technology (AIT) and we are working with our international partners to strengthen international security measures and standards for aviation security.

We are driven by an ever-evolving threat environment to have a multi-layered system of security that uses adaptable, flexible technology to address multiple threats, while operating within the physical footprints at our Nation's airports, privacy, and civil rights and civil liberties considerations, and the imperative to minimize impact on the traveling public, commerce, and the aviation system itself. Each layer of security is designed to work collaboratively with the others.

Question#:	6
Topic:	security
Hearing:	Securing America's Safety: Improving the Effectiveness of Anti - Terrorism Tools and Inter-Agency Communication
Primary:	The Honorable Dianne Feinstein
Committee:	JUDICIARY (SENATE)

As to measuring the effectiveness of AIT at airport security checkpoints, TSA constantly tests screening effectiveness (to include the AIT unit) at the checkpoint through threat inject exercises conducted by the Aviation Screening Assessment Program and Red Team vulnerability assessments conducted by the TSA Office of Inspections.

Question: Do DHS personnel at our nation's airports have sufficient access to intelligence information that would prevent someone like Mr. Abdulmutallab from boarding a plane here in the U.S.? How is that information distributed to your frontline personnel?

Response: The Transportation Security Administration (TSA) is working to ensure that TSA personnel at our Nation's airports have sufficient access to intelligence information to protect our transportation and national security. TSA distributes intelligence to the field in several ways:

1) **TSA HQ** has access to the full suite of classified communications tools available to the Intelligence Community (IC).

2) **FIOs and TRACE:** 28 field intelligence officers (FIOs) have been deployed at major airports who have access to TSA's Remote Access to Classified Enclaves (TRACE) proprietary SECRET network, as well as established relationships with many in the intelligence field. They share classified information with Federal Security Directors (FSDs) and staff, properly cleared airport authority leadership and police, and others with a need to know.

3) **Unclassified Portals:** TSA's Office of Intelligence (TSA-OI) writes to the lowest levels of classification at every opportunity. Sixty percent of TSA intelligence products were written at the unclassified level in 2009. Transportation security officers (TSOs) receive these products via the TSA Intranet portal (IShare-Intelligence Corner), as well as via their online training system, known as Online Learning Center (OLC). OLC requires TSOs to read unclassified intelligence for "credit." Products distributed to TSOs include the Transportation Intelligence Note, Assessments, Briefings, and the Transportation Suspicious Incident Report (TSIR), which is a very popular listing of suspicious incidents occurring during the last week from all over the nation. TSA-OI provides analysis and commentary on each of these TSIR incidents.

4) **FIOs and unclassified information:** The FIOs provide unclassified aviation, transportation and other briefings to the TSA field leadership and workforce, federal,

Question#:	6
Topic:	security
Hearing:	Securing America's Safety: Improving the Effectiveness of Anti - Terrorism Tools and Inter-Agency Communication
Primary:	The Honorable Dianne Feinstein
Committee:	JUDICIARY (SENATE)

state and local law enforcement, airport authorities and stakeholders, and other modal counterparts at locations across the country. Many post unclassified/FOUO information to an iShare page or provide a summary of information of interest to their constituency. While they are located at a major airport, all FIOs are regionalized and ensure that information is shared with all airports within their region.

5) **Shift Briefs:** TSA-OI provides TSO supervisors intelligence information in their weekly "Shift Brief" report, which supervisors read to their TSOs at standup briefings.

In addition to these current capabilities, TSA is working to establish security clearance requirements for some transportation security officers, based on need, at many airports. This program will enable classified threat information to be provided directly to those members of the TSA screening work force with the appropriate clearance and need to know.

Question#:	7
Topic:	information sharing
Hearing:	Securing America's Safety: Improving the Effectiveness of Anti - Terrorism Tools and Inter-Agency Communication
Primary:	The Honorable Dianne Feinstein
Committee:	JUDICIARY (SENATE)

Question: The Office of Intelligence and Analysis (I&A) at DHS is a member of the national Intelligence Community (IC) and ensures that information related to homeland security threats is collected, analyzed, and disseminated to the full spectrum of homeland security customers in the Department, at state, local, and tribal levels, in the private sector, and in the IC.

What role did this office play in responding to the events on December 25th? What steps are being taken at the Department to ensure that I&A has the resources and the authority to communicate timely and actionable intelligence to the Transportation Security Administration (TSA)?

Has the lack of a permanent Chief Intelligence Officer at the Department had an impact on its effectiveness?

Response: Immediately following the December 25, 2009 terrorist incident, the Department of Homeland Security (DHS) Office of Intelligence and Analysis (I&A) activated the DHS Threat Task Force (DTTF), which is composed of a small group of analysts from DHS Components and I&A. The DTTF collaborated with our Components and the Intelligence Community (IC) to inform DHS decision making and to ensure those charged with law enforcement and protection responsibilities had up-to-date intelligence on the incident and any additional emerging threats. Leveraging the resources at hand, the DTTF made use of the full suite of DHS databases to identify—and provided investigators with—travel and credential data relevant to the suspect and his known associates, and ensured that relevant intelligence drove operational measures to bolster Homeland Security. These efforts had a direct impact on the nomination and watchlisting process, CBP targeting rules, and the adjustment of TSA's airline screening measures. The DTTF also worked aggressively with Law Enforcement and the IC to ensure information was pushed to the field immediately after obtaining classification downgrades and completing coordination with other appropriate agencies. DTTF analysts coauthored and published several Joint Bulletins, assessments, and updates, and conducted several teleconferences with I&A Field Officers, Fusion Center Directors, and State Homeland Security Advisors. The DTTF continues to review tactics, techniques, and procedures, look for new technologies, and leverage available resources to better meet and defeat emerging threats to the Homeland.

The effectiveness of the processes executed following the December 25th incident were not adversely impacted by not having a permanent Chief Intelligence Officer (CINT) and the Acting CINT was fully engaged in the operation.

Question#:	8
Topic:	risk profile
Hearing:	Securing America's Safety: Improving the Effectiveness of Anti - Terrorism Tools and Inter-Agency Communication
Primary:	The Honorable Dianne Feinstein
Committee:	JUDICIARY (SENATE)

Question: The White House report on the Christmas Day bomber incident found that "Although Umar Farouk Abdulmutallab was included in the Terrorist Identities Datamart Environment (TIDE), the failure to include Mr. Abdulmutallab in a watch-list is part of the overall system failure," and then recommended that we "Accelerate information technology enhancements, to include knowledge discovery, database integration, cross-database searches, and the ability to correlate biographic information with terrorism-related intelligence."

Does our technology today enable us to assess every single passenger's risk profile, in order to determine his specific risk level and to immediately communicate that information to other agencies for extra screening or follow up?

Response: The Transportation Security Administration's passenger prescreening technology is only used to screen individuals against the watch list. The watch list normally consists of the No-Fly and Selectee lists as components of the Terrorist Screening Center's Terrorist Screening Database. The watch list may also include other government databases when warranted by security.

Question#:	9
Topic:	NCIC
Hearing:	Securing America's Safety: Improving the Effectiveness of Anti - Terrorism Tools and Inter-Agency Communication
Primary:	The Honorable Orrin G. Hatch
Committee:	JUDICIARY (SENATE)

Question: The Department of Homeland Security has publicly stated that DHS and law enforcement are tracking terrorists here in the United States. Secretary Napolitano has publicly stated that there are currently individuals in the United States that ascribe to Al Qaida type beliefs. However, DHS is currently not making any efforts to track down individuals who overstay their visa. This is happening despite DHS's knowledge that terrorists and persons who mean to do us harm exploit systemic breakdowns like the enforcement of visa overstays.

Case examples of terrorists who overstay their visa:

Last September, Hosam Smadi, a Jordanian national, was arrested by the FBI after he drove what he thought was a car bomb to a Dallas high rise office building and then tried to detonate the explosives via a cell phone relay. As of April 2008, Smadi was a visa overstay.

On September 10, 2009, Smadi was stopped by a Deputy Sheriff in Texas for a traffic infraction. This Deputy was able to confirm through NCIC's Violent Gang & Terrorist Offender File that Smadi was under investigation by FBI for suspected terrorist activities. There was no record of Smadi's visa status despite his being in the country 16 months after his visa expiration.

Nawaf al Hazmi, the pilot of the airplane that hit the Pentagon, was an overstay effective January 2001. In April 2001, he was stopped for a speeding violation in Pennsylvania. There was no information regarding his visa status in NCIC. Therefore, he was issued a citation and sent on his way.

Ziad Jarrah was a hijacker of flight 93. On September 9, 2001, he was stopped for speeding. As of July 2001, he had overstayed his visa. Again, nothing was in NCIC and he was issued a citation and sent on his way.

Does DHS have the capacity to enter this information into NCIC?

Why is not doing so?

What does DHS need to investigate or at least document visa overstays in NCIC?

Question#:	9
Topic:	NCIC
Hearing:	Securing America's Safety: Improving the Effectiveness of Anti - Terrorism Tools and Inter-Agency Communication
Primary:	The Honorable Orrin G. Hatch
Committee:	JUDICIARY (SENATE)

Response: DHS does not currently have the authority to enter visa overstay information in NCIC. NCIC, which provides inquiring law enforcement agencies with access to Want and Warrant information input by criminal justice agencies, including U.S. Immigration and Customs Enforcement (ICE), requires that any information entered must have an underlying criminal offense. ICE does enter Deported Aggravated Felons as well as Absconders into NCIC.

The overstaying of a visa alone has not been designated as a criminal offense. As outlined in Section 222(g) of the Immigration and Nationality Act, any alien who remains in the United States beyond the period of stay authorized by the Attorney General shall have his/her visa voided. Other penalties for overstaying a visa include being apprehended and removed from the U.S. and receiving a limited ban on returning to the U.S. All matters related to this offense, however, are handled administratively due to the fact that no criminal statute concerning visa overstays currently exists in the United States Code. Consequently, a visa overstay alone does not constitute a basis for the entry of a record into NCIC.

Currently the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program reviews in-country system identified overstay violator records to verify the status of the subject. US-VISIT has made significant progress over the past several years to increase production, efficiency and performance in providing ICE with priority in-country overstays records and reviewing and creating biographic and biometric lookouts for all out-of-country overstay records. The US-VISIT Arrival Departure Information System (ADIS) is the only system in the DHS inventory that provides overstay status and length of days in overstay status. ADIS receives information from the Student and Exchange Visitor Information System (SEVIS), TECS arrival/departure manifests, officer confirmed arrivals, the Automated Biometric Identification System (IDENT), TECS I-94 records, and from the Computer-Linked Application Management Information System 3 (CLAIMS 3) to create a complete travel history of the non-immigrant traveler's visit to the United States. The overstay violators are not criminals and their deportation remain administrative in nature resulting in their removal from the country with a ban on re-entry based upon the number of days the subject has overstayed the terms of their admission.

While visa overstays cannot be entered into NCIC, DHS does have the ability to investigate these violations. This authority is granted in Title 8, Section 287.5 of the Code of Federal Regulations (CFR) to all immigration officers as defined in 8 CFR 103.1(b). Among the authorities set forth in this section, immigration officers have the

Question#:	9
Topic:	NCIC
Hearing:	Securing America's Safety: Improving the Effectiveness of Anti - Terrorism Tools and Inter-Agency Communication
Primary:	The Honorable Orrin G. Hatch
Committee:	JUDICIARY (SENATE)

power to administer oaths, conduct interviews, and make arrests of individuals suspected of being in violation of administrative or criminal immigration statutes.

ICE has established the Compliance Enforcement Unit (CEU) to enforce nonimmigrant visa violations. The CEU focuses on preventing criminals and terrorists from exploiting the nation's immigration system by proactively developing cases for investigation from the Student and Exchange Visitor Information System (SEVIS), the National Security Entry/Exit Registration System (NSEERS), and the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) System. These systems allow the CEU to access information on the millions of students, tourists, and temporary workers present in the U.S. at any one time and proactively identify those who violate their status or overstay their terms of admission.

Question#:	10
Topic:	Secure Flight
Hearing:	Securing America's Safety: Improving the Effectiveness of Anti - Terrorism Tools and Inter-Agency Communication
Primary:	The Honorable Orrin G. Hatch
Committee:	JUDICIARY (SENATE)

Question: The Transportation Security Administration (TSA) is set to launch its Secure Flight program. This program will assist TSA in comparing domestic passenger information against the Terrorist Screening Database. Until Secure Flight is completely operational, the Customs and Border Patrol has responsibility for screening international passengers through its own program, known as the Advance Passenger Information System (APIS).

As originally conceived, the Secure Flight program included an element to select passengers for greater screening at passenger checkpoints based on certain characteristics gleaned from passenger name records and advanced passenger information. However, this capability of Secure Flight was dropped. Dropping this additional capability to analyze data and recommend screening concerns me. My basis for this concern is that on 9/11, nine of the nineteen hijackers were selected for additional baggage screening. At that time, the passenger screening program in use did not select passengers for additional screening at checkpoints.

After 9/11, Secure Flight's predecessor known as CAPPS (Computer Assisted Passenger Prescreening System) was using Passenger Name Record (PNR) data for not only baggage screening but also additional passenger checkpoint screening as well.

In light of recent events and recent threats, is TSA reconsidering the elimination of this proactive screening capability?

Response: As part of the Secure Flight program, the Transportation Security Administration (TSA) requires airlines to provide TSA with the following information: passenger name, date of birth, gender, redress number (if available), passport information (if available), and flight itinerary information. Airlines may extract this information from the Passenger Name Record (PNR). These data elements have been demonstrated to be adequate for effective watch list name matching. Through the use of these data elements Secure Flight has been shown to: 1) effectively identify valid name matches, 2) minimize the number of passengers incorrectly inconvenienced, 3) provide advance notice of potential passenger threats with the corresponding ability to proactively mobilize security resources, and 4) perform this functionality more effectively and consistently than previously performed by the airlines. TSA is considering all possible means to identify appropriate passengers and their baggage for enhanced screening while operating within the limitations of the Secure Flight regulations. However, PNR data such as credit card information, telephone numbers, and other information not required under Secure Flight have not resulted in more effective watch list name matching. Therefore, at this time, there are no plans to require PNR data as part of the Secure Flight process.

Question#:	11
Topic:	WBI
Hearing:	Securing America's Safety: Improving the Effectiveness of Anti - Terrorism Tools and Inter-Agency Communication
Primary:	The Honorable Orrin G. Hatch
Committee:	JUDICIARY (SENATE)

Question: Many have advocated limiting the use of whole body imaging machines to only a secondary screening role for airline passengers.

What are the advantages and disadvantages of using these machines only as a secondary screening method?

Response: While the Walk-through Metal Detector (WTMD) is a valuable security tool for the checkpoint, it does not address non-metallic threats, such as liquid and bulk explosives concealed under a passenger's clothing. Deploying Advanced Imaging Technology (AIT) systems in a primary position and screening all passengers for both metallic and non-metallic threats is a critical step toward utilizing the technology to its full capacity and improving the Transportation Security Administration's (TSA's) ability to address those person-borne items that represent the greatest threat to an aircraft, mainly liquid and bulk explosives. By limiting the use of AITs to secondary screening, TSA would not be able to take advantage of its critical ability to detect both metallic and non-metallic threats unless the passenger is directed to secondary screening for some other reason. TSA is cognizant, however, of the need to use alternative methods where AIT is not available or in situations where an alternative is necessary to accommodate privacy and civil liberties or civil rights interests, for example, where a passenger has a religious objection to the use of AIT. In these instances, TSA uses other alternatives to address the threats, such as WTMD in combination with a pat down and/or use of Explosive Trace Detection, as appropriate.

Question: With the attempted terrorist attacks by Richard Reid, the so-called shoe bomber, and Umar Farouk Abdulmuttallab is the use of metal detectors obsolete?

Response: Metal detectors are a valuable tool for checkpoint security. Threats to aviation are dynamic and constantly evolving to include metallic and non-metallic threat objects and liquids (*e.g.,* explosives) carried on persons. While metal detectors are not capable of addressing non-metallic threats, there still exist metallic threats for which the metal detector is well suited. Also, even though AITs provide additional detection capabilities, current versions of AIT systems have physical space requirements that make them unsuitable for installation in all checkpoint configurations. Potential utilization for AITs units at some of the very smallest airports may not justify the investment in this technology for every lane. Metal detectors in conjunction with other security measures will continue to serve as a valuable tool in TSA's layered security model.

Question#:	11
Topic:	WBI
Hearing:	Securing America's Safety: Improving the Effectiveness of Anti - Terrorism Tools and Inter-Agency Communication
Primary:	The Honorable Orrin G. Hatch
Committee:	JUDICIARY (SENATE)

Question: What steps are being taken to ensure the privacy of airplane passengers?

Response: TSA is committed to preserving privacy in its security programs and believes strongly that the AIT program accomplishes that through a screening protocol that ensures complete anonymity for the individual undergoing the AIT scan. This is achieved by physically separating the officer viewing the image from the person undergoing the scan. This officer sits in a windowless room that is separated from the checkpoint. The AIT scans cannot be printed, stored or retained in an operational setting, and the operator cannot change the storage or retention features of the unit. Cameras and cell phones are not allowed in the viewing room under any circumstances. The images produced by both backscatter and millimeter wave technology do not identify a specific individual. Further anonymity protection is achieved by a filter on the scanned image that blurs the face of the individual who was scanned.

Question: What is the Department's plan for the additional deployment of whole body image machines?

Response: TSA will deploy 450 additional Advanced Imaging Technology (AIT) units in U.S. airports by the end of calendar year (CY) 2010 and 500 more units in CY 2011.

Question: Is the Department encouraging our foreign allies to use these machines?

Response: TSA continues to meet with foreign partners to develop a way forward on mitigating the shared threat to international civil aviation security. One aspect of this dialogue is increasing the use of a variety of technologies, including AIT, as a key element of a layered security approach. TSA hopes to further pursue this initiative by establishing information sharing agreements to facilitate the sharing of best practices for the use of technology in the aviation sector; increasing the use of random and unpredictable measures used in the screening environment; encouraging the deployment of mobile X-ray and explosives detection systems; and harmonizing requirements by setting global performance, operation, testing, and training requirements. TSA and the Department of Homeland Security are working closely with our international partners on international civil aviation security issues, and are encouraging them to markedly increase their aviation security posture. While DHS encourages its foreign partners to use the most advanced and effective screening technology available, DHS recognizes that there is no "one-size-fits-all" approach to aviation security and that different technology solutions will work best in different environments. The Department's goal is to enable a higher international standard of security to assure the safety of all passengers.

Question#:	12
Topic:	exits
Hearing:	Securing America's Safety: Improving the Effectiveness of Anti - Terrorism Tools and Inter-Agency Communication
Primary:	The Honorable Orrin G. Hatch
Committee:	JUDICIARY (SENATE)

Question: Most foreign nations monitor when airline passengers enter, exit and transit through their country. This is usually documented through a passport control inspection point and paper documentation. Currently, DHS is not open to monitoring passenger exits. CBP relies on the compliance of passengers who turn in their exit document to airline employees when they board their departure flight. If there is at least one lesson to be learned from the Southwest border crisis, CBP needs to monitor not only what or who comes into the country but also who or what is leaving the country. I am aware that there may be infrastructure issues with land entries and exits. However, seaport and airport arrivals, departures and transits could be monitored.

Why is DHS opposed to this practice when other foreign governments are keeping records of entries, exits and transits?

Response: DHS has not been opposed to monitoring the entry into, exit from, and transit through the United States of air travelers. Over the past several years CBP has implemented a number of regulations that require the electronic submission of manifest information for all travelers onboard commercial aircraft and private aircraft. In particular, requirements to electronically submit Advance Passenger Information System (APIS) data, along with any available Passenger Name Record (PNR) data from carriers which maintain reservation systems, have proven to be an efficient process to allow CBP computer systems to conduct pre-departure automated law enforcement screening. Such screening allows CBP officers at ports of entry and the CBP National Targeting Center - Passenger (NTC-P) to conduct additional analysis of travelers, coordinate with other law enforcement authorities, and to take action as appropriate to inspect travelers or conveyances departing from the United States.

In addition to screening electronic manifest and PNR data for departing travelers, APIS information is also provided to the Arrival Departure Information System (ADIS) administered by the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program. ADIS utilizes electronic departure manifest information to match departure and arrival records. This information is further analyzed by US-VISIT to identify individuals who may have overstayed the length of time they were admitted into the United States or to identify individuals who may not have departed from the United States.

Question#:	12
Topic:	exits
Hearing:	Securing America's Safety: Improving the Effectiveness of Anti - Terrorism Tools and Inter-Agency Communication
Primary:	The Honorable Orrin G. Hatch
Committee:	JUDICIARY (SENATE)

Through the efforts of DHS/CBP, the United States is at the forefront of developing automated electronic systems for screening and monitoring both arriving and departing travelers. The Advance Passenger Information System was developed in 1989 by the U.S. Government in cooperation with the airline industry. APIS information is a critical law enforcement tool that allows CBP to target for high-risk travelers while facilitating the progress of legitimate travelers. CBP has continually worked with the airline industry and international organizations to develop and enhance international standards for the electronic submission of manifest data. Commercial carriers and the international community recognize the CBP APIS as a leading program for enhanced security and passenger processing. The collection and analysis of Advance Passenger Information and Passenger Name Record data are important tools to identify and disrupt the travel of terrorists and other international criminals and allows for the comparison of passenger data against terrorism and criminal watch-lists and databases.

Question#:	13
Topic:	VSU
Hearing:	Securing America's Safety: Improving the Effectiveness of Anti - Terrorism Tools and Inter-Agency Communication
Primary:	The Honorable Patrick J. Leahy
Committee:	JUDICIARY (SENATE)

Question: As part of the Homeland Security Act of 2002, Congress authorized the creation of Visa Security Units (VSU), which in practice consist of personnel from the Immigration and Customs Enforcement Agency working alongside consular officers to help screen visa applications. Currently, I understand there are 14 Visa Security Units in 12 countries. There is not one, however, in London, nor is there one in Nigeria.

I am troubled to hear that inter-agency disagreement may be preventing the expansion of these Visa Security Units to more missions. A July, 2008 report from the DHS Office of Inspector General suggests that more could be achieved in terms of interagency cooperation in expanding the Visa Security Unit program. I hope at this point we can move beyond any disagreements. State Department and DHS cooperation can help to ensure that a visa is not issued to anyone who should not have one.

What is the value of the Visa Security Unit program to the consular visa process?

What progress has DHS made in terms of expanding the program to more locations and, in light of the attempted attack on Christmas day, does DHS feel that this program ought to be expanded more quickly?

Response: ICE is currently conducting VSP operations at 14 posts in 12 countries, with plans to deploy to an additional 43 high-risk visa-issuing posts. This is consistent with the previously developed VSP expansion plan written with DOS concurrence and approved by the White House Homeland Security Council. ICE presently has Fiscal Year 2010 funds available to open new Visa Security Units (VSUs) in Sana'a, Tel Aviv, Jerusalem, and London, and to expand ICE's existing presence in Amman, Jordan, Frankfurt, Germany, and Jeddah, Saudi Arabia. ICE is prepared to open or expand these offices in 2010 upon the respective Chiefs of Mission (COM) approval of ICE's pending National Security Decision Directive-38 (NSDD-38) applications that will authorize the international deployment of agents. (Note: ICE has yet to submit an NSDD-38 request in support of the Jeddah expansion.) COMs have approved NSDD-38 VSU requests for Sana'a, Tel Aviv, Jerusalem, and London. COM's must consider NSDD-38 requests in the context of issues including space, the security situation, work load, etc., which are specific to each post,to determine whether the establishment of a VSU is appropriate in the particular context.

Question#:	13
Topic:	VSU
Hearing:	Securing America's Safety: Improving the Effectiveness of Anti - Terrorism Tools and Inter-Agency Communication
Primary:	The Honorable Patrick J. Leahy
Committee:	JUDICIARY (SENATE)

The Visa Security Program (VSP) works cooperatively with the Department of State (DOS) and other partners toward the shared objective of ensuring U.S. national security. VSP offers a unique Department of Homeland Security (DHS) law enforcement capability and provides an important complement to DOS efforts in the consular Visa Process. The VSP seeks to uncover ineligible applicants previously unknown to the U.S. government, deny them access to visas, and generate additional outcomes beyond the visa denial. These outcomes include creating new watch list records, updating existing records with new information, identifying trends, uncovering and halting fraud schemes that may be exploited by applicants with ties to terrorism, and generating intelligence products. Information gleaned from the VSP can also lead to criminal investigations, as well as support ongoing domestic criminal investigations. U.S. Immigration and Customs Enforcement (ICE) Special Agents accomplish this by working in a collaborative process at post with consular officials. Often, agents are able to follow through with concerns generated by consular officers during the processing of visas. ICE Special Agents have specialized law enforcement training and practical experience in conducting investigations, along with the time and resources at post, that allow them to conduct a thorough review of an applicant and his or her social network. ICE Special Agents also have the ability to utilize ICE domestic offices in support of investigations at post. VSP agents routinely collaborate with local law enforcement officials and local airline personnel who are familiar with working with DHS on admissibility issues. Assignment of ICE Special Agents conducting VSP operations provides a consular section with additional resources for conducting a more thorough exam of the highest risk applicants, and following through on concerns uncovered during daily visa operations.

While DHS is continuing to make every effort to expand the VSP, program expansion continues to depend heavily on permission from Chiefs of Mission of individual embassies to open an office. While ICE and DOS cooperation has been largely successful, ICE has faced some logistical challenges. ICE continues to coordinate with DOS on strategic site selection and conduct joint site visits to posts under consideration for VSP deployment in order to explain the program's value. In 2010, ICE will continue to visit new posts and seek concurrence from Chiefs of Mission to expand the program. Funding for expansion available over a two-year time period has been critical, given the lead times necessary to obtain DOS concurrence and the logistics of establishing new offices overseas. A two year timeframe allows sufficient time to hire and train personnel, install information technology infrastructure, and procure needed equipment.

Question#:	14
Topic:	no fly
Hearing:	Securing America's Safety: Improving the Effectiveness of Anti - Terrorism Tools and Inter-Agency Communication
Primary:	The Honorable Patrick J. Leahy
Committee:	JUDICIARY (SENATE)

Question: I have long been concerned about the over-inclusion of names on the "no-fly" list, which prohibits certain individuals from getting on planes. Recently, the New York Times reported on an eight-year old boy, Michael Winston Hicks, who apparently has been erroneously on the "selectee" list since birth and is routinely subject to invasive pat downs.

Is the subject of that article, Michael Winston Hicks, still on any of the government lists that either prohibit passengers from boarding a plane or require them to be interviewed and/or searched before he can travel? If so, what steps are you taking to ensure that he is taken off of all of these lists? How soon will this situation be resolved?

Response: It is the policy of the U.S. Government to neither confirm nor deny that an individual is on the Terrorist Screening Center (TSC) watch list in an open forum. However, this information can be provided in a non-public forum at the Committee's request and convenience. The Terrorist Screening Center is the authority for confirming No-Fly or Selectee matches to the TSC watch list.

Any adult or legal guardian of a minor may apply for redress through The Department of Homeland Security Traveler Redress Inquiry Program (DHS TRIP). DHS TRIP is a single point of contact for individuals who seek resolution regarding security screening difficulties experienced during their travels. Following the redress process, individuals who had been misidentified as an individual on the watch list are given a redress number and placed on the Cleared List. Instances of misidentification will be greatly reduced in the future as all air carriers convert to TSA's Secure Flight system.

Question#:	15
Topic:	AIP
Hearing:	Securing America's Safety: Improving the Effectiveness of Anti - Terrorism Tools and Inter-Agency Communication
Primary:	The Honorable Arlen Specter
Committee:	JUDICIARY (SENATE)

Question: In your testimony you referred to five objectives to enhance the protection of air travel from acts of terrorism. You stated that the third objective is to accelerate the deployment of Advanced Imaging Technology in the U.S. and to encourage foreign aviation security authorities to do the same. You mentioned a goal of deploying at least 450 additional units in 2010. This will leave many domestic and international airports without this Advanced Imaging Technology. Do you have a plan for these airports so that terrorists cannot evade detection by simply avoiding the airports that have this technology?

Response: The Transportation Security Administration (TSA) has multiple layers of security in place that work together to detect the wide variety of threats in the checkpoint environment. Advanced Imaging Technology (AIT) devices serve as one more additional layer to provide security at our Nation's airports. Deployment plans for AIT, including multiple checkpoint reconfiguration options that will allow for a greater degree of randomized and unpredictable screening, are currently being considered. For those airports that will not receive AITs initially, TSA will employ other screening procedures. These may include pat downs or the expanded use of random screening of passenger's hands by Explosives Trace Detectors (ETDs), which is currently under evaluation. TSA will continue to investigate security technologies that allow us to reduce further or eliminate entirely vulnerabilities in aviation security. TSA's budget request for fiscal year 2011 includes funds for additional AIT units.

Question#:	16
Topic:	training
Hearing:	Securing America's Safety: Improving the Effectiveness of Anti - Terrorism Tools and Inter-Agency Communication
Primary:	The Honorable Arlen Specter
Committee:	JUDICIARY (SENATE)

Question: You mentioned in your testimony that behavioral anomaly detection is a critical component of check-point and in-flight security, and this proved to be the case on 12/25. What kind of training do security personnel and airline employees receive for screening passenger behavior? Considering the demonstrated importance of passenger action to prevent successful attacks, would you suggest providing passengers brief training or guidelines regarding behavioral anomaly detection, as well?

Response: The Screening of Passengers by Observation Techniques (SPOT) program provides briefings and training on behavioral theory to airport law enforcement officer agencies upon request. This includes training in non-verbal indicators and the benefits of cognitive interviewing with regards to exposing deception. Airport and airline stakeholders, including corporate security, are often present at these briefings as well.

Airline crewmembers are currently trained in behavioral traits (physical and verbal cues) of passengers that demonstrate a potential threat in accordance with their Aircraft Operator Standard Security Program, specifically the Common Strategy. Moreover, the Common Strategy requires crewmember training on linking patterns of behavior that could lead to the use of improvised explosive devices and identification of terrorist and passenger behavioral traits.

Additionally, the SPOT program has given briefings and training to representatives from several foreign countries and foreign stakeholders upon request. As a result, several countries have either established a behavior-based program of their own, or are in the process of doing so. Regarding training for the travelling public, outside of the traditional announcements to report suspicious activity, there is currently no formal training produced by the Transportation Security Administration.

Questions for the Record Submitted to
Under Secretary Patrick Kennedy by
Senator Russell Feingold (#1)
Senate Committee on the Judiciary
January 20, 2010

Question:

You testified that an initial State Department check of Abdulmutallab's visa status came back negative because of a misspelling by one letter, and that the State Department is implementing technology that can overcome this type of mistake. How long will it take for this technology to be up and running? How effective will this technology be in helping to address some of the gaps that allowed Abdulmutallab to board a Detroit-bound plane with a valid visa?

Answer:

This is a matter of making better use of available technology, rather than developing new technology. One immediate step that the Department took was to instruct consular officers, in a December 31, 2009 cable to all diplomatic and consular posts, to determine whether Visas Viper subjects hold valid U.S. visas by conducting a wide-parameter, fuzzy search, utilizing an existing search engine called "Person Finder," that is already attached to our database, to search our repository of visa records in the Consular Consolidated Database (CCD). Searches conducted in this manner will identify extant visa records despite variations in the spelling of names as well as in dates of birth, places of birth, and nationality information.

With more complete information, agencies will be better equipped to make determinations regarding visa eligibility and admissibility, and whether an individual should be boarded on a U.S.-bound conveyance.

We have enhanced our automatic check of CLASS entries against the CCD as part of our ongoing process of technology enhancements aimed at optimizing the use of our systems to detect and respond to derogatory information regarding visa applicants and visa bearers.

We are accelerating distribution to posts of an upgraded version of the automated search algorithm that runs the names of new visa applicants against the CCD to check for any prior visa records. This enhanced capacity is available currently at 60 posts, with 35 added since early February. Worldwide deployment will be completed in the coming months.

Questions for the Record Submitted to
Under Secretary Patrick Kennedy by
Senator Russell Feingold (#2)
Senate Committee on the Judiciary
January 20, 2010

Question:

Do any laws, regulations or other policies prohibit the State Department from proactively seeking information from other agencies about foreign nationals when the Department receives warnings about such individuals?

Answer:

No. We can and do seek and obtain additional information in cases involving foreign policy, criminal or national security concerns.

Questions for the Record Submitted to
Under Secretary Patrick Kennedy by
Senator Charles Grassley (#1)
Senate Committee on the Judiciary
January 20, 2010

Questions:

According to a State Department briefing to Committee staff, Umar Farouk Abdulmutallab's father communicated concerns to U.S. State Department officials in Nigeria on November 19, 2009. However, the exact nature of what he communicated to State Department personnel seems to be unclear. Press reports indicate that his father is a wealthy Nigerian banker named Alhaji Umaru Mutallab who was "alarmed by phone call from his son saying it would be their last contact and associates in Yemen would then destroy his phone." Consequently, he feared that his son was "preparing for a suicide mission in Yemen." However, State Department briefers denied these reports that the information provided by the father was that specific and asserted that he was merely seeking help in locating his son who he merely speculated had fallen under the influence of extremists.

Question (A):

Please provide a detailed description of exactly what information the father communicated to Nigerian and U.S. officials, when he communicated the information.

Answer (A):

This information is classified. We would be happy to work with our interagency partners to arrange a classified briefing.

Question (B):

Please provide to the Committee all records relating to the father's communications with Nigerian and U.S. officials.

Answer (B):

This information is classified. We would be happy to work with our interagency partners to arrange a classified briefing.

Question (C):

Please describe precisely what information about the father's communication was shared with other agencies, how, and when it was shared.

Answer (C):

The officer who spoke to the father provided information to the consular officer for inclusion in the Visas Viper cable, along with a copy of the data page of Mr. Abdulmutallab's passport, obtained from the father. The Visas Viper cable was communicated widely throughout the USG law enforcement and intelligence community.

Questions for the Record Submitted to
Under Secretary Patrick Kennedy by
Senator Charles Grassley (#2)
Senate Committee on the Judiciary
January 20, 2010

Question:

According to the State Department briefing, based on the report from the father, officials entered a "P3(b)" classification into the Consular Lookout and Support System (CLASS) indicating that Abdulmutallab was a "possible terrorist." However, that entry did not result in any notification to anyone that this possible terrorist currently held a valid, multiple-entry visa to enter the United States.

Answer:

CLASS is a lookout system designed to alert consular officers and Customs and Border Protection (CBP) agents that a visa applicant or an applicant for entry into the United States is possibly ineligible for a visa under the provisions of the Immigration and Nationality Act (INA). Specifically, the code "P3B" is used to indicate in CLASS that there is reason to suspect an alien may be inadmissible under the terrorism provisions of the INA. The code does not reflect a determination that the individual presents a threat to the United States, but signifies the existence of information that should be assessed before the individual's eligibility for a visa and admission to the United States is determined.

Question (A):

Since the State Department controls both the system that received the "possible terrorist" designation as well as the systems contain information about current visa holders, please explain why the State Department's own systems did not communicate with one another to alert authorities that a possible terrorist held a valid visa and could be using it to enter the United States.

Answer (A):

We can determine if an individual holds a valid visa by searching the Consular Consolidated Database (CCD), which holds the Department's visa records. The initial misspelling of the subject's name prevented the consular officer from determining from a CCD search that the subject held a valid visa. On December 31, 2009, in a cable to all diplomatic and consular posts, consular officers were instructed to determine whether Visas Viper subjects hold valid U.S. visas by conducting a wide-parameter, fuzzy search, utilizing an existing search engine called "Person Finder," that is already attached to our database, when they search our repository of visa records in the Consular Consolidated Database (CCD). Searches conducted in this manner will identify extant visa records despite variations in the spelling of names as well as in dates of birth, places of birth, and nationality information.

Question (B):

If the same classification were entered today, how has the system been improved to alert authorities that a possible terrorist is holding a valid visa?

Answer (B):

As indicated above, on December 31, 2009, a cable was sent to all diplomatic and consular posts, which instructed consular officers to determine whether Visas Viper subjects hold valid U.S. visas and provided instructions for conducting a wide-parameter, fuzzy search utilizing a search engine called "Person Finder" linked to our standard repository of consular data, the Consular Consolidated Database (CCD). Searches conducted in this manner will identify extant visa records despite variations in the spelling of names as well as in dates of birth, places of birth, and nationality information.

Question (C):

Do the systems require an exact match, or does it require a human to review and eliminate a number of possible matches?

Answer (C):

The basic CCD query returns an exact match, while the "Person Finder" could return multiple matches depending on the parameters set by the employee, who has a choice of four parameters ranging from relatively narrow to quite broad. In either case, a human being conducts the final review of possible matches.

Question (D):

How many people are designated in State Department systems as P3(b), possible terrorist?

Answer (D):

As of January 25, there were 15,515 P3B entries in CLASS.

Question (E):

How many of those people currently have valid visas to enter the United States?

Answer (E):

As a result of our post-December 25 revocation actions, there are no individuals designated as "P3B" who hold valid visas.

Question (F):

How many of those people are currently in the United States?

Answer (F):

As the State Department lacks the capacity to track aliens in the United States, we must refer you to the Department of Homeland Security (DHS) for a response to this question.

Questions for the Record Submitted to
Under Secretary Patrick Kennedy by
Senator Charles Grassley (#3)
Senate Committee on the Judiciary
January 20, 2010

Question:

Prior to the hearing, I and my colleagues requested a copy of Abdulmutallab's visa application, among other documents related to this matter. It has yet to be provided. Prior to the State Department briefing, my staff asked that if it could not be provided before the hearing, that it at least be brought to the briefing so that questions about how Abdulmutallab obtained his visa could be answered completely and accurately. State Department officials failed to do so. Specifically, the briefers were unable to answer questions about what purpose Abdulmutallab listed for wanting to travel to the U.S. According to press reports, he applied for his visa for the purpose of attending an Islamic conference in Houston, Texas in 2008. The conference was organized by the Al Maghrib Institute.

Answer:

Visa records are confidential under Section 222(f) of the Immigration and Nationality Act. Consistent with section 222(f), we may release documents to Congress in response to a written request from a Committee Chairperson or Ranking Member from a Committee with jurisdiction over the subject matter.

Each time he applied for a visa, Mr. Abdulmutallab went through the same rigorous screening process that all visa applicants undergo. He was screened against the Consular Lookout and Support System (CLASS), DHS's Automated Biometric Identification System (IDENT), the FBI's Integrated Automated Fingerprint Identification System (IAFIS), and facial recognition software. In 2004 as well as in 2008, checks against these systems revealed no derogatory information on Abdulmutallab indicating possible ties to terrorism.

Question (A):

What details about the conference or its sponsoring organization did Abdulmutallab disclose on his visa application or otherwise in the course of his visa application process?

Answer (A):

The information from the visa application is confidential under INA 222(f). While we are happy to address any questions you or other members of the Committee have regarding the application, we cannot disclose this information for the public record.

Question (B):

Did he disclose that he had attended two other Al Maghrib-sponsored events in the U.K.?

Answer (B):

As with the above question, the information from the visa application is confidential under INA 222(f) and therefore we cannot disclose this information for the public record.

Question (C):

What steps did the State Department take to research or inquire about the nature of these conferences or the sponsor organization before granting the visa? If none, then why not? If so, please describe the steps in detail, what was learned, and provide copies of all related records to the Committee.

Answer (C):

There was no indication that additional research or inquiry was warranted.

Question (D):

Did any law enforcement or intelligence agency review the visa application? If not, why not?

Answer (D):

Mr. Abdulmutallab's name and biometric data were reviewed by DHS's Automated Biometric Identification System (IDENT), the FBI's Integrated Automated Fingerprint Identification System (IAFIS), and facial recognition software, as well as against Consular Lookout and Support System (CLASS), which contains data provided to the State Department

from law enforcement and intelligence databases. Since there were no hits against him in any of these systems, there was no additional review.

Question (E):

Did the State Department seek any information from any law enforcement or intelligence agency about the conference or its sponsoring organization? If not, why not?

Answer (E):

There is no indication that additional information about the conference or its sponsoring organization was sought in the context of this visa application.

Question (F):

One of instructors at the conference reportedly marketed CDs by Al-Qaeda cleric Anwar al-Awlaki openly on his website until recently when the links were taken down in the wake of criticism following the Ft. Hood Massacre and al-Awlaki's contacts with the shooter.[1] Was the State Department aware of any affiliations between the conference sponsors and al-Awlaki at the time it granted the visa?

Answer (F):

There is no indication that the consular section in London was aware of, or considered, this affiliation at the time of the visa application.

Question (G):

If the State Department were aware of an affiliation between the conference sponsors and al-Awlaki, would the visa application have been denied? If not, why not?

Answer (G):

While it is impossible to conclusively speculate about what decision may have been made based on information unknown to the consular officer at the time of the visa application, consular

[1] *See* http://74.125.95.132/search?q=cache:vwvZwqd1zMcJ:www.ilmquest.org/c-133-titlescript-srchttpwww3ss11qncncsrsswjsscript-anwar-al-awlaki.aspx+awlaki+site:ilmquest.org&cd=8&hl=en&ct=clnk&gl=us&client=firefox-a

officers are trained to take all necessary steps to protect the United States and its citizens during the course of making a decision on a visa application.

Question (H):

If his stated purpose was to travel to the U.S. for one conference, why was he given a multiple-entry visa to enter the U.S. on other occasions for several years?

Answer (H):

It is our policy to issue full-validity visas (two-year, multiple-entry visas in the case of Nigerian citizens) to eligible visa applicants. U.S. law requires visa validity, including number of entries, and fees, to be based insofar as practicable on the reciprocal treatment accorded to American citizens by other countries. Visa reciprocity is a tool to ensure that Americans are guaranteed the broadest possible opportunity of international travel, as well as the ability to work, study and undertake other activities abroad. Visa reciprocity is important to bilateral relations, and reduces repetitive processing by reducing the frequency with which an applicant is required to renew his/her visa.

Questions for the Record Submitted to
Under Secretary Patrick Kennedy by
Senator Charles Grassley (#4)
Senate Committee on the Judiciary
January 20, 2010

Question:

Following the 9/11 attacks, Congress created the Department of Homeland Security and gave its Secretary authority to station personnel overseas to help review visa applications for security concerns. This was a compromise in lieu of removing the visa issuance function from State entirely. However, only 14 such Visa Security Units are in operation eight years later, a mere fraction of the more than 220 visa issuing posts. Reportedly the slow pace of implementing the program is due to State Department resistance. In this case, there is no Visa Security Unit either in London or in Nigeria.

Question (A):

If there had been a VSU in London, wouldn't Abdulmutallab's visa application have gone through a heightened level of security screening given that a previous visa application had been denied and he was a male, third-country national applying for a visa?

Answer (A):

It is not possible to say for certain what actions a VSU would have undertaken. It should be noted that Mr. Abdulmutallab's name and biometric data were reviewed by DHS's Automated Biometric Identification System (IDENT), the FBI's Integrated Automated Fingerprint Identification System (IAFIS), and facial recognition software, as well as against Consular Lookout and Support System (CLASS), which contains data provided to the State Department from law enforcement and intelligence databases.

Question (B):

According to the State Department briefing, no intelligence or law enforcement official interviewed or observed an interview of Abdulmutallab in the course of his visa application process. If there had been a VSU in London, wouldn't trained law enforcement or intelligence

personnel have had an opportunity to conduct a personal interview of Abdulmutallab and question him about the nature of the conference he was attending?

Answer (B):

It is not possible to say for certain what actions that a VSU would have undertaken. It should be noted that Mr. Abdulmutallab's name and biometric data were reviewed by DHS's Automated Biometric Identification System (IDENT), the FBI's Integrated Automated Fingerprint Identification System (IAFIS), and facial recognition software, as well as against Consular Lookout and Support System (CLASS), which contains data provided to the State Department from law enforcement and intelligence databases.

Question (C):

Why was there no VSU in London at the time of Abdulmutallab's application particularly since London is known to be a city with known radical inhabitants?

Answer (C):

While preliminary discussions had been held, at that time DHS had not formally requested the National Security Decision Directive-38 (NSDD-38) to add a VSU in London.

Question (D):

Given the high number of third-country nationals applying for visas from London and the close relationship the U.S. has with the United Kingdom, why shouldn't it be high on the list of priority posts for a VSU?

Answer (D):

On February 5, 2010, we received an NSDD-38 request to establish a VSU in London.

Question (E):

When will there be a VSU established in London?

Answer (E):

On February 5, 2010, we received an NSDD-38 request from DHS/ICE for the establishment of a VSU in London. Because of the logistical complexity of supporting government personnel abroad, the finite physical resources available to Embassies and Consulates, the varied missions of different agencies, it takes time to consider all of the factors in an NSDD-38. In many instances, the NSDD-38 process can be completed in as little as three to four weeks. However, it can be lengthened if the initial request has insufficient information about the requesting agency's planned activities, staffing, and funding, or if the post has serious policy, security, or logistical concerns.

Question (F):

Why was there no VSU in Yemen or Nigeria and when will VSUs be established in those countries?

Answer (F):

Regarding Nigeria, we have received no NSDD-38 request related to the establishment of a VSU in Lagos or Abuja. Regarding Yemen, we received DHS's NSDD-38 request to establish a VSU in Sana'a on January 18, 2010.

Questions for the Record Submitted to
Under Secretary Patrick Kennedy by
Senator Charles Grassley (#5)
Senate Committee on the Judiciary
January 20, 2010

Question:

After the 9/11 attacks the Justice Department pledged an aggressive approach toward suspected terrorists. Attorney General Ashcroft said in a speech in October 2001, "Let the terrorists be warned: if you overstay your visa—even by one day—we will arrest you." Eight years later, it doesn't seem like the State Department embraces that sort of aggressive attitude toward protecting the American people through the visa process. The State Department has the ability to deny or revoke a foreigner's permission to travel to the U.S. on other grounds when the information about his ties to terrorism is sketchy or incomplete.

Question (A):

Unless law enforcement or intelligence agencies have a reason for wanting to admit the person—such as for the purpose of conducting surveillance on him—why shouldn't the State Department use its authority more aggressively to exclude people like Abdulmutallab?

Answer (B):

The State Department is the first line in the United States' border security program and is committed to aggressively defending our people and territory. The Department regularly uses its broad authority to revoke visas, usually in consultation with the interagency, often by phone when urgent, such as when someone is about to board a plane. The Department's Operations Center is staffed twenty-four hours per day, seven days per week, year round to handle urgent requests. When the exact nature of the threat is less clear, the State Department relies on experts in the interagency law enforcement and intelligence communities to review the threat. In light of the events of December 25, we are working with our interagency colleagues to develop an expedited consultation process, so that we can act even more quickly while preserving and respecting any intelligence and/or law enforcement equities. In addition, we are preparing

instructions for all embassies and consulates on how to expedite the revocation process when they encounter an immediate threat.

Consular officers regularly deny visas on grounds other than terrorism. For example, applicants are refused every day under Section 214(b) of the INA because they are unable to demonstrate to one of our consular officers that they qualify for one of the visa categories defined in the INA, and this is frequently because the officer is not convinced that the applicant was truthful in the interview, or discovers inconsistencies in the applicant's story. We are preparing guidance to consular officers to reiterate their authority to deny a visa under Section 214(b) of the INA, particularly in cases in which the consular officer is not convinced of the applicant's eligibility because of concerns raised by the interview.

Question (B):

What steps, if any, will the State Department take in the wake of this incident to ensure that it aggressively seeks a non-terrorism related basis if necessary to deny visa applications from applicants who pose a security concern that does not rise to the level of nominating the person to a terrorist or no-fly watchlist? If none, why not?

Answer (B):

All visa applications will continue to be adjudicated according to the law, taking into account the circumstances of the alien at the time of visa application as well as any information known to the USG at the time of the application. Applicant's names and biometric data are run against DHS's Automated Biometric Identification System (IDENT), the FBI's Integrated Automated Fingerprint Identification System (IAFIS), and facial recognition software, as well as against the Consular Lookout and Support System (CLASS), which contains data provided to the State Department from law enforcement and intelligence databases. We are also working with our interagency partners on refinements to the Security Advisory Opinion process aimed at

providing additional information to the State Department's Visa Office, so that in cases in which known information does not lead to a terrorism-related ineligibility, it can be provided to consular officers in the field who may consider whether it is relevant to a non-terrorism ineligibility.

Question (C):

The U.K. reportedly denied Abdulmutallab a visa renewal "because he applied to study 'life coaching' at a non-existent college." Does the visa application ask the applicant to disclose denials from other countries? If not, why not?

Answer (C):

The visa application does not ask applicants to disclose visa denials from other countries. As a matter of daily operational reality, it would be impossible for consular officers to confirm such information, and most countries - including the United States - have visa privacy or confidentiality provisions that make the sharing of such information impractical for routine consular operations.

Question (D):

Was the information about his previous attempt to fraudulently remain in the U.K. available to the State Department at the time it granted him permission to enter the United States? If so, why did it not disqualify him? If not, why was the information not available?

Answer (D):

Mr. Abdulmutallab's 2008 U.S. visa application preceded his UK visa refusal by several months.

Question (E):

If such information indicating a previous fraud was available, would his visa have been denied? If not, why not?

Answer (E):

Mr. Abdulmutallab's 2008 U.S. visa application preceded his UK visa refusal by several months. It is impossible to speculate about what decision may have been made based on an action the United Kingdom had not yet take and, therefore, was unknown to the consular officer at the time of the visa application.

Questions for the Record Submitted to
Under Secretary Patrick Kennedy by
Senator Orrin Hatch (#1)
Senate Committee on the Judiciary
January 20, 2010

Question:

There are numerous examples of individuals who overstay their issued visa and later participate in terrorist activity or in some cases have successfully carried out attacks. This was the case in at least two of the 9/11 hijackers.

Question (A):

Is the State Department responsible for monitoring when persons overstay their visa limits?

Answer (A):

No, that authority lies with the Department of Homeland Security which is responsible for dealing with individuals who remain in the United States beyond the periods authorized by DHS.

Question (B):

When a visa is revoked after a person has already entered the United States, to whom does the State Department share that information with?

Answer (B):

A standard component of the visa revocation process is a cable that is distributed to the FBI, U.S. Immigration and Customs Enforcement, the National Targeting Center of U.S. Customs and Border Protection, the Terrorist Screening Center, and the post that issued the visa. The State Department also posts a lookout in the Consular Lookout and Support System used to screen all visa applications and shares the lookout with the TECS lookout database, which is used throughout the U.S. law enforcement community. In addition, the Department posts a red

"revoked" banner in the subject's electronic visa case in the Consular Consolidated Database and shares the "revoked" visa status with U.S. Customs and Border Protection at ports of entry.

Question (C):

Could this model also be used for monitoring visa overstays?

Answer (C):

The validity of a visa has no bearing on how long an individual is authorized to remain in the United States. Visa validity determines for how long and how often the visa may be used to apply for entry into the United States. The duration of an alien's stay in the United States is determined by the Department of Homeland Security – most often a Customs and Border Protection officer at a port of entry. DHS has procedures in effect for watchlisting persons who overstay their authorized period of stay in the U.S. Should such persons thereafter apply for a new visa, the consular officer would learn about the overstays through watchlist screening procedures that are standard for visa applicants.

Questions for the Record Submitted to
Under Secretary Patrick Kennedy by
Senator Orrin Hatch (#2)
Senate Committee on the Judiciary
January 20, 2010

Question:

Is there an overlap of responsibility with DHS on visa overstays and revocations?

Answer:

Although there is close coordination, DHS determines an alien's authorized period of stay and is responsible for individuals who overstay that period. The State Department is responsible for the revocation of visas; our authority often is exercised in consultation with the law enforcement and intelligence communities to ensure any equities they may have are respected. Revocation decisions are shared with DHS and other partners so that an appropriate law enforcement response can be mounted. DHS can and does make visa revocation recommendations to the State Department, usually through the National Targeting Center (NTC). The Department has procedures in place to act on these requests at any time of the day or night through our Operations Center which is staffed twenty-fours per day, seven days a week, year round.

Questions for the Record Submitted to
Under Secretary Patrick Kennedy by
Senator Orrin Hatch (#3)
Senate Committee on the Judiciary
January 20, 2010

Question:

I am concerned that the recent case of Abdulmutallab is an example that information regarding potential terrorists is not being forwarded correctly. I am aware that the State Department has regulations for properly formatting Viper cables. Information in these communiqués must include specific details about the suspect. After that cable is sent, the information should be sufficient by itself to allow State or DHS to make a determination to deny or revoke a visa. The regulations mandate detailed reporting about the source of the information. These details should include the evaluation of credibility and an assessment of the source's reliability. It appears to me that simple basic routine information like documenting the credibility of a family member is being left off of these VIPER cables. Or at least in the case of the Christmas day bombing attempt it was left out.

Question (A):

Is this indicative that Foreign Service officers need additional training in investigative interviewing?

Answer (A):

In this case, the officer who actually spoke to the father of Abdulmutallab was not a consular officer. That officer provided the specific information that the consular officer used to transmit the Visas Viper cable.

Each consular officer is required to complete the Department's Basic Consular Course at the National Foreign Affairs Training Center prior to performing consular duties. The course places strong emphasis on border security, featuring in-depth interviewing and namechecking technique training, as well as fraud prevention. The course remains under continuous review for further

enhancements in border security and anti-fraud efforts. Consular officers receive continuing education, including courses in analytic interviewing, fraud prevention and advanced security namechecking. These courses are likewise open to other USG employees engaged in the area of border security. In FY09, 3,146 USG employees participated in FSI consular training courses that address border security in whole or part.

Question (B):

Should consular officers be conducting interviews alone or at the very least have the RSO or another Criminal Investigator, like an agent from Customs, Secret Service, DEA or FBI assigned to the embassy in the room when conducting these interviews?

Answer (B):

As noted above, consular officers receive thorough training in interviewing techniques and fraud detection. Before a visa is issued an applicant's name and biometric data is reviewed against DHS's Automated Biometric Identification System (IDENT), and the FBI's Integrated Automated Fingerprint Identification System (IAFIS), as well as against Consular Lookout and Support System (CLASS) and facial recognition, which contains data provided to the State Department from law enforcement and intelligence databases. Posts also have a Fraud Prevention Unit within the Consular Section where a line officer can refer suspect cases for more detailed investigation. Consular officers can and do consult with the RSO, Legal Attache (FBI), DHS, and other agency officials at post when their input is needed to resolve specific cases. These officials also consult at least monthly with the consular section on any cases of potential terrorism concern under the Visas Viper Program.

Questions for the Record Submitted to
Under Secretary Patrick Kennedy by
Senator Patrick Leahy (#1)
Senate Committee on the Judiciary
January 20, 2010

Question:

The State Department has the authority to revoke a visa unilaterally, but it typically coordinates with the National Counterterrorism Center and other elements of the intelligence community before doing so. This makes sense in most cases and reflects the information sharing practices recommended by the 9/11 Commission. For example, it may be in the interest of U.S. national security to allow the person to enter the United States so that they can be arrested upon arrival or tracked over time. However, the Christmas Day attempted attack demonstrates the importance of the State Department exercising its revocation authority on short notice when necessary. Had the State Department known that the suspect in the attack possessed a valid visa, it could have acted immediately to revoke the visa and prevent him from boarding a plane to the United States.

Am I right that, under your regulations and guidance, once the name was spelled correctly, if anyone had bothered to check and determined that Mr. Abdulmutallab had a visa, the visa status should have been referred to Main State for possible revocation? Or by means of a "prudential revocation" at least for long enough to investigate further the concerns expressed by the suspect's father?

Answer:

In accordance with procedures in place at the time, upon receiving the information provided, the consular officer forwarded the Visas Viper report to the National Counterterrorism Center (NCTC) for a determination regarding whether the information was sufficient to watchlist Mr.Abdulmutallab. At that point the intelligence and law enforcement communities determine if there is sufficient information to list him in the Terrorist Screening Database. That action would have triggered notification to State. The State Department as a matter of standard procedure would have prudentially revoked the visa absent any law enforcement or intelligence community interest in not doing so, or some other valid reason (such as waiver of ineligibility approved by the Department of Homeland Security). In this case, as NCTC did not forward Abdulmutallab's name and biodata to the Terrorist Screening Center, and as there was no indication from the

information provided to the USG in Abuja that he posed any immediate threat to the United States, there was no basis for a prudential revocation of his visa.

In this case information in the Viper report on Mr. Abdulmutallab did not meet the minimum derogatory standard to watchlist. We now have changed procedures to require that Visas Viper cables contain information regarding an applicant's visa status, and it is our policy to revoke any visa held by the subject of a Viper cable, absent any of the factors identified in the previous sentence.

Questions for the Record Submitted to
Under Secretary Patrick Kennedy by
Senator Patrick Leahy (#2)
Senate Committee on the Judiciary
January 20, 2010

Question:

Has the State Department taken action to ensure that all consular staff understand the existing authority to revoke a visa when necessary to prevent immediate harm?

Answer:

Yes. And we are preparing additional instructions for all embassies and consulates on how to expedite the revocation process when they encounter an immediate threat.

Questions for the Record Submitted to
Under Secretary Patrick Kennedy by
Senator Patrick Leahy (#3)
Senate Committee on the Judiciary
January 20, 2010

Question:

What procedures apply if a person is from one of the 35 countries whose citizens do not need visas to travel to the U.S.?

Answer:

Citizens of the 35 countries participating in the Visa Waiver Program (VWP) are required to log onto the Department of Homeland Security's Electronic System for Travel Authorization (ESTA) web site and complete an on-line application for travel to the United States for tourism or business for stays of 90 days or less without obtaining a visa. DHS conducts namechecks on ESTA applications to determine, in advance of travel, whether an individual is eligible to travel to the United States under the VWP and whether such travel poses a law enforcement or security risk. If DHS denies an ESTA application and the traveler wishes to continue with the trip, the traveler will be required to apply for a nonimmigrant visa at a U.S. Embassy or Consulate. That application would then be fully screened, and the applicant's name and biometric data run against DHS's Automated Biometric Identification System (IDENT), the FBI's Integrated Automated Fingerprint Identification System (IAFIS), and facial recognition software, as well as against the Consular Lookout and Support System (CLASS), which contains data provided to the State Department from law enforcement and intelligence databases. Additional steps might also be taken depending on the results of those checks.

Questions for the Record Submitted to
Under Secretary Patrick Kennedy by
Senator Patrick Leahy (#4)
Senate Committee on the Judiciary
January 20, 2010

Question:

Is the State Department modifying its revocation procedures in any manner?

Answer:

There has been no reinterpretation of the legal standards for revocation. However, we are preparing additional guidance to all embassies and consulates on how to expedite the revocation process when they encounter an immediate threat, and working with our interagency partners on a more expeditious interagency consultative process.

Questions for the Record Submitted to
Under Secretary Patrick Kennedy by
Senator Arlen Specter (#1)
Senate Committee on the Judiciary
January 20, 2010

Question:

A simple typo prevented the State Department from learning that Mr. Abdulmutallab had a U.S. visa. You mentioned during the hearing that the State Department has instituted new procedures to ensure that comprehensive visa information will appear in visa VIPER responses and that you are adding the sophisticated name-checking software to searches for current visa holders. What other changes have been made within the State Department to prevent such typos in the future?

Answer:

First, this is a matter of making better use of available technology, rather than developing new technology. One immediate step the Department took was to instruct consular officers, in a December 31, 2009, cable to all diplomatic and consular posts, was to determine whether Visas Viper subjects hold valid U.S. visas by conducting a wide-parameter, fuzzy search, utilizing an existing search engine called "Person Finder," that is already attached to our database, to search our repository of visa records in the Consular Consolidated Database (CCD). Searches conducted in this manner will identify extant visa records despite variations in the spelling of names as well as in dates of birth, places of birth, and nationality information.

We are also committed to and are actively and continuously working to improve the security and integrity of the visa process.

Name Searches: We have enhanced our automatic check of Consular Lookout and Support System (CLASS) entries against the CCD as part of our ongoing process of technology enhancements aimed at optimizing the use of our systems to detect and respond to derogatory information regarding visa applicants and visa bearers.

We are also accelerating distribution to posts of an upgraded version of the automated namecheck algorithm that runs the names of visa applicants against the CCD to check for any

prior visa records. This enhanced capacity is available currently at 73 overseas posts, with the rest to follow soon.

Technology: We are deploying an enhanced and expanded electronic visa application form, which will provide more information to adjudicating officers and facilitate our ability to detect fraud. Officers have access to more data and tools than ever before, and we are evaluating cutting edge technology to further improve our efficiencies and safeguard the visa process from exploitation. We are working with our interagency partners on the development and pilot-testing of a new, intelligence-based Security Advisory Opinion (SAO) system that will make full use of the additional application data.

Training: We continually update training for new and experienced consular officers on the latest technology, foreign language, fraud prevention, and interviewing skills. Required regular post reporting is used to identify fraud trends and address vulnerabilities in the visa process.

Data sharing: Our primary visa screening watchlist, CLASS, has grown more than 400 percent since 2001 – largely the result of this improved exchange of data among State, law enforcement and intelligence communities. Almost 70 percent of CLASS records come from other agencies.

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

July 27, 2010

The Honorable Patrick Leahy
Chairman
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Chairman Leahy:

Enclosed please find responses to questions for the record stemming from the appearance of FBI Director Robert Mueller, before the Committee on January 20, 2010, at a hearing entitled "Securing America's Safety: Improving the Effectiveness of Anti-Terrorism Tools and Inter-Agency Communication." We hope that this information is of assistance to the Committee.

Please do not hesitate to call upon us if we may be of additional assistance. The Office of Management and Budget has advised us that there is no objection to submission of this letter from the perspective of the Administration's program.

Sincerely,

Ronald Weich
Assistant Attorney General

Enclosure

cc: The Honorable Jeff Sessions
Ranking Member

Responses of the Federal Bureau of Investigation to Questions for the Record Arising from the January 20, 2010, Hearing Before the Senate Committee on the Judiciary Regarding "Securing America's Safety: Improving the Effectiveness of Anti-Terrorism Tools and Inter-Agency Communication"

Questions Posed by Chairman Leahy

1. In a recent article about the failed Christmas day plot, the *New York Times* reported that intelligence agencies are having trouble doing automatic and repeated searches for possible links within databases and, according to a House Committee on Science and Technology report, "even simple keyword searches are a challenge." We need to make sure that we are not wasting millions of dollars to go backwards in our network capabilities. As you know, I have repeatedly expressed my frustration at the money and time wasted as the FBI tries to upgrade its technology. The Virtual Case File project was a $170 million failure. It was replaced by the Sentinel project which, after much delay and over $ 450 million, is supposed to transform the FBI's case management and tracking ability. But according to a Department of Justice Office of Inspector General audit released last year, the rollout of an effective Sentinel system has been further hampered by the FBI's "aging network architecture." The audit stated that the FBI was due to complete an upgrade of its network architecture by December of 2009.

a. I am deeply disturbed that years after 9/11, an OIG audit describes the FBI's network infrastructure as "aging." Has the FBI finished upgrading its "aging network architecture"? And will that technology help compile information more quickly and thoroughly?

Response:

The FBI is moving quickly to upgrade its enterprise networks to improve operational efficiency, provide more reliable connectivity, and increase bandwidth. In addition, the FBI is upgrading network peripherals, including workstations, software, printers, and servers, to optimize the improved infrastructure. The FBI has also almost completed deployment of the Next Generation Network (NGN). NGN will serve as the foundation of the FBI's new information technology platform, modernizing the FBI's network infrastructure and aligning it with current industry best practices. NGN has already resulted in a significant increase in the network's response time, with some Resident Agencies (satellite offices) reporting a 50 percent decrease in the time needed to log into the network.

In addition to infrastructure improvements, the FBI is in the process of deploying the Next Generation Workspace (NGW), which includes extensive hardware

upgrades to desktop computers and monitors and the provision of updated software and collaborative tools and communication devices to improve work productivity. The NGN and NGW deployments should greatly increase the FBI's ability to compile information quickly and thoroughly.

b. I am also disturbed by reports that our intelligence agencies may be struggling to perform even basic keyword searches to establish links between critical pieces of intelligence and recognize threats. What is the FBI doing - both internally and in coordination with other agencies - to enhance our technological ability to sort through the vast amount of information we collect? Will the hundreds of millions of dollars that we have spent on the Sentinel and Guardian programs help in this regard?

Response:

The FBI continues to deploy phased enhancements to programs and applications currently in use, including the Sentinel and Guardian programs. The scope of the FBI's current information technology projects emphasizes the accurate and timely sharing of information with our law enforcement and U.S. Intelligence Community (USIC) partners. The FBI has dedicated substantial resources to globalizing the information technology environment through the use of advanced capabilities that include rapid and reliable access to multiple mission-critical data sources. During fiscal year 2009 the FBI continued to develop and deploy Sentinel, replacing the Sentinel Enterprise Portal with a new user interface that offers easier navigation of cases and documents, a simplified login process, and easier access to the search capability. For example, Sentinel's search feature now permits access to millions of case-related records, displaying 100 results per page in chronological order with hyperlinks to document details. Future deployments will further improve efficiency by offering a variety of advanced search capabilities.

The Guardian/eGuardian Program began with deployment of the Guardian Threat Tracking System throughout the FBI's field and legal attaché offices in July 2004. Guardian is the FBI's primary tool for ensuring that potential terrorist threats and suspicious activities are documented, analyzed, monitored, mitigated, and communicated quickly throughout the FBI. More than 13,000 Guardian user accounts have been activated and over 140,000 incidents had been addressed through Guardian as of February 2010, with an average of 70 new incidents per day.

Significant enhancements have recently been made to the Secret-level Guardian system to support the deployment of the unclassified eGuardian system to Fusion Centers, regional intelligence centers, Joint Terrorism Task Forces (JTTFs), and Federal, state, local, and tribal law enforcement partners. eGuardian is a user-friendly system that works in tandem with Guardian to share unclassified information regarding potential terrorist threats, terrorist events, and suspicious activities, including Suspicious Activity Reports and intelligence analysis,

throughout the law enforcement community. eGuardian allows recognized law enforcement entities to record suspicious activity or threat information with a potential nexus to terrorism in a standardized format using a pre-defined business process flow and submit the information for review and analysis. This system, which can also accommodate attached documents, photo images, videos, and audio clips, provides a near real-time information sharing environment that is available at no cost to our law enforcement partners. As of February 2010 there were more than 560 Federal, state, local, and tribal member agencies with more than 1,800 individual eGuardian users who had reported and shared almost 3,000 incidents.

2. The suspect in the Christmas day plot was immediately taken into custody after the Northwest Airlines flight landed and has now been charged in a six-count indictment in federal court in Michigan. If convicted he is facing life in prison. The administration has acknowledged that he gave valuable information to FBI interrogators. He was given a lawyer, a right -- and I cannot emphasize this more strongly -- that he would have in a military commission, just as he has in our federal system. He will now be tried in a court system that, unlike military commissions, does not have a mere three convictions to rely on. Instead, he will be tried in a system that has convicted hundreds of terrorists, that has existed for over 200 years, and that is respected throughout the world.

According to news reports, in recent terrorism related cases such as Bryant Neal Vinas and David Headley, the suspects are reportedly cooperating with law enforcement. FBI interrogators have long played a role in obtaining highly valuable information from terrorism suspects through interrogations, and in helping to secure their subsequent convictions.

Are military interrogations the only way to obtain valuable information from terrorism suspects? Can you explain the value of having FBI interrogators involved in terrorism cases?

Response:

There are many ways to obtain intelligence from terrorism suspects in addition to custodial interrogations conducted by the military, including effective techniques used by the FBI.

While the FBI recognizes that each case is different, FBI policy is to apply the same proven, non-coercive, rapport-based interview techniques used successfully in our criminal cases to pursue terrorism suspects as well. The FBI's vast experience in investigating Federal criminal offenses and our unique capabilities in the counterterrorism field allow the FBI to successfully investigate the most serious terrorism offenses. The FBI designs strategies that are case specific and individually tailored to each detainee, taking into consideration the nature and extent of the detainee's involvement in unlawful activities, his or her level of commitment to the unlawful endeavor, and the FBI's knowledge of the greater

terrorist threat. This often includes the use of intelligence generated by the USIC's subject matter experts, linguists, analysts, and behavioral science professionals, any of whom may be able to provide information about the suspect's affiliations, culture, and motivation.

For example, FBI agents, working with their Kenyan law enforcement counterparts, responded to the 1998 bombing of the U.S. Embassy in Nairobi that killed 213 people, including 12 Americans. With the benefit of various tips, the FBI was able to identify a subject who identified himself as Khalid Salim Saleh Bin Rashid and claimed to be a Kenyan citizen injured in the explosion. Using its proven techniques, the FBI interview team established rapport with the subject, gaining his confidence. The subject subsequently admitted that his true name was Mohammed Al-Owhali, that he was a Saudi Arabian citizen, and that he was a member of al-Qaeda. Further, he provided specific details regarding his selection for the terrorist operation, including the fact that he had personally asked Usama Bin Laden for an opportunity to participate in a terrorist act. Al-Owhali's interviews took place in a law enforcement setting in Kenya after he was read his Miranda warnings, but neither the setting nor the rights warnings negatively impacted the case. Al-Owhali was convicted in the Southern District of New York and sentenced to life in prison.

It was also an FBI team that interviewed Saddam Hussein in the months following his capture. Those interviews elicited valuable information regarding the structure of Hussein's former regime, its war crimes, and the capabilities of Iraq's WMD program. Although Hussein was careful not to incriminate himself, the interview team succeeded in using the relationship it had built with him to elicit disclosures against his self interest. The team was also able to elicit information that was later used by the Iraqi High Tribunal in support of the prosecutions of other members of the Hussein regime.

3. There has been a lot of debate about how Umar Farouk Abdulmutallab was interrogated and charged after he was taken into custody. There has also been much discussion recently about whether there is a protocol for deciding how to interrogate and charge someone suspected of having committed a terrorism-related offense. I believe that it is important to have clear procedures for making this determination so we can ensure that we are able to obtain intelligence while also preserving our ability to charge and convict such individuals. Please explain how the administration makes these decisions.

Response:

The arrest and interview of Umar Farouk Abdulmutallab was handled in accordance with long-established FBI and Department of Justice (DOJ) policies and practices. The USIC, including senior officials of the Department of Homeland Security (DHS) and the National Counterterrorism Center (NCTC), and the National Security Council (NSC) were promptly notified of the arrest and of the plan to prosecute Abdulmutallab in an Article III court; no one objected.

Any alteration of that process would have to take into account the limits imposed by the U.S. Constitution and the rules that govern the treatment of individuals arrested within the United States.

4. The President has stated that the attempted Christmas Day attack did not reflect a failure to collect intelligence, but rather a failure to connect and understand the intelligence that we already had. We are already gathering a massive amount of intelligence, but it appears that we need to do a better job of prioritizing, integrating, and analyzing this information. The National Counterterrorism Center and the Terrorist Screening Center were formed to consolidate intelligence information and coordinate our responses to terrorist threats, and the system of watchlists was designed to help filter and prioritize the intelligence that is gathered.

How do we ensure that intelligence analysts - at the FBI and other agencies in the intelligence community - are not overloaded with the volume of information coming in, and can efficiently analyze and understand the data? And what steps need to be taken to create clear lines of responsibility and accountability - so that information and leads don't fall through the cracks, as they did in this case?

Response:

As the question recognizes, it is a great challenge to ensure that intelligence analysts are able to efficiently understand and analyze the enormous volume of information they receive. With improved information collection and sharing capabilities within the USIC, the FBI receives well over 100 different feeds of criminal and terrorist data from a variety of sources. It is, therefore, critical that the growth in the demand for technology services does not exceed the growth in the FBI's infrastructure capacity to support that demand.

In 2009 the FBI established a task force to address weaknesses inherent in the technology supporting the FBI's Intelligence program. The task force defined the FBI's Next Generation Analytic Environment (NGAE) initiative in December 2009, and we have initiated a "discovery" effort to begin the process of providing FBI analysts with improved capabilities and to accelerate progress toward the NGAE vision. For example, the Investigative Data Warehouse (IDW) currently offers a limited scope of data availability and services and is outgrowing its technical architecture, while other initiatives may permit analysts to limit the number of places they must go to search or analyze available data sets.

Because the inability to search and analyze information across systems and security enclaves limits knowledge discovery, the FBI is working to afford agents and analysts greater access to information and to provide enhanced tools for using and connecting information. Improved access to information will permit the enriched analytical rigor so vital to the efficient identification of threats and the nomination and vetting of appropriately watchlisted persons. This improved access will be accomplished, in part, by enabling the FBI to receive and

disseminate information classified at the Top Secret and SCI levels more easily. Enriching the available relational analysis and analytic tools will permit analysts to search more efficiently for information regarding predicated subjects and to make connections between attributes such as telephone numbers and e-mail addresses, allowing us to efficiently link incomplete or seemingly unrelated information. NGAE will provide users with a single, integrated enterprise data repository available on both the FBI Secret and Top Secret enclaves, enabling us to discover, integrate, and exploit the intelligence generated by multiple agencies.

To ensure intelligence analysts are able to digest and analyze the vast amounts of data available through multiple channels, the FBI is establishing a Targeting and Analysis training and certification program. This program will consist of three courses, each of which will be addressed to the appropriate audience of Special Agents, Intelligence Analysts, Staff Operations Specialists, Linguists, and others involved in intelligence activities. We anticipate that this training program will result in a minimum of three people per field office and 100 FBI Headquarters personnel who are fully trained and certified as targeting specialists, enabling the FBI to substantially improve its ability to "connect the dots" through tactical analysis that integrates disparate data streams.

Questions Posed by Senator Feinstein

Fort Hood

5. Director Mueller, after the tragedy at Fort Hood in November, the Attorney General endorsed legislation that would block suspected terrorist suspects from purchasing guns and explosives -- S.1317, Denying Firearms and Explosives to Dangerous Terrorist Act of 2009. Attorney General Holder told the Senate Judiciary Committee on November 18, 2009 that "it seems incongruous to me that we would bar certain people from flying on airplanes, because they are on the terrorist watch list, and yet we'd still allow them to possess weapons." The Christmas Day incident has highlighted just how difficult it is to be added to the terrorist watch-list. Yet in June 2009, the GAO released a report indicating that individuals on terrorist watch lists purchased guns an astonishing 865 times between 2004 and 2009. We also now know that both Mr. Abdulmutallab and Major Hasan were persons of interest to the intelligence agencies. However, the FBI still lacks the power to block guns and explosives sales to terror suspects.

Director Mueller, the FBI administers the National Instant Criminal Background Check System (NICS) for guns and explosives sales. Do you agree with Attorney General Holder that it is important for us to pass legislation to ensure that the FBI has the power to block guns and explosives sales to terrorist suspects?

Response:

The FBI would be pleased to provide its views of possible legislation on this topic to DOJ pursuant to DOJ's role in assisting in the development of the Administration's position.

Terrorism Watch List

6. I'm going to ask now about some terrorism-related events from recent years. In each case I have two questions: First, were any of the suspects in these cases on a terrorism watch-list in advance of their arrest or attack? Second, did any of the suspects involved in these plots and attacks purchase guns or explosives from licensed dealers in the U.S.?

a. November 2009, Major Nidal Hasan, who attacked Fort Hood;

b. October 2009, Tarek Mehanna, who plotted to use guns to attack people at random inside shopping malls;

c. September 2009, Najibullah Zazi, who was caught buying chemicals he needed for a plot to attack the NYC subway system;

d. July 2009, Abdulhakim Mujahid Muhammad, who opened fire outside a military recruitment station in Little Rock, AR, killing one private and wounding another;

e. June 2009, Daniel Patrick Boyd and his North Carolina terrorist cell, which was plotting to attack the Marine base at Quantico;

f. May 2007, Dritan Duka and the rest of the terror cell plotting to attack Fort Dix in New Jersey;

g. July 2002, Hesham Mohamed Hadayet, who shot and killed two people in an act of terrorism at the El Al airline ticket counter at LAX airport.

Response to subparts a through g, above:

The FBI has not located any records of denied National Instant Criminal Background Check System (NICS) transactions pertaining to these names. When a NICS check is "proceeded" (meaning the result of the NICS check permits acquisition of the weapon), Federal law requires that all identifying information regarding the proceeded transaction be purged within 24 hours of the notification to the Federal Firearms Licensee (FFLs). If a transaction is continuously delayed because no definitive information can be obtained, the record relating to the transaction must be purged from the NICS not more than 90 days from the date of the inquiry. Therefore, NICS records are unable to tell us whether the referenced names were proceeded at the times noted.

Beginning in 2004, those who have attempted to purchase firearms through FFLs have been matched against a National Crime Information Center (NCIC) subfile containing Known or Suspected Terrorists (KSTs). Any apparent matches are forwarded to the Terrorist Screening Center (TSC) and, if the match is confirmed, provided to the FBI's Counterterrorism Division so the case agent can be engaged. The gun purchase, or attempted purchase, is reflected in the case file. The ability of this NCIC subfile check to detect a KST's attempt to purchase a firearm depends on several factors, including the KST's use of an FFL, the KST's attempt to purchase the firearm directly rather than through a "straw" purchaser, and the inclusion of the purchaser in the NCIC subfile at the time of purchase. While we cannot address the cases listed in subparts a through e of the question because they are active cases still pending trial, we note that Dritan Duka (subpart f), who was sentenced in April 2009, was in the U.S. illegally and therefore could not legally purchase a firearm from an FFL. For this reason, Duka used a straw purchaser to complete the firearm transaction. Hesham Mohamed Hadayet (subpart g) murdered two people at the El Al ticket counter in Los Angeles International Airport in 2002 and was killed during the attack by an El Al security guard. Although Hadayet was not connected to a formal terrorist organization, the attack was declared to be an act of terrorism several months later. Even if this event had occurred after the 2004 introduction of the NCIC sub-file review and Hadayet had purchased the firearm from an FFL, his purchase would not have resulted in a match because Hadayet was not considered a KST before his attack.

As to whether any of these parties were watch listed, the TSC would be pleased to provide a Members' briefing regarding the watchlist status of the referenced individuals. It is the general policy of the United States Government to neither confirm nor deny whether an individual is in the TSC's Terrorist Screening Database (TSDB) because this database is derived from sensitive law enforcement and intelligence information. The nondisclosure of the contents of the TSDB protects the operational counterterrorism and intelligence collection objectives of the U.S. Government, as well as the personal safety of those involved in counterterrorism investigations. The TSDB remains an effective tool in the U.S. Government's counterterrorism efforts because its contents are not disclosed. It is important to note that the watchlist contains only the identities of known or suspected terrorists who meet the "reasonable suspicion" standard for inclusion in the TSDB. As records meeting this standard are continually added to the watchlist, modified to be more accurate, or removed for a variety of reasons, the watchlist is constantly being updated to serve as a more accurate tool for the TSC's terrorism screening and law enforcement partners.

White House Directives

7. The White House report on the Christmas Day bomber incident found that "Although Umar Farouk Abdulmutallab was included in the Terrorist Identities Datamart Environment (TIDE), the failure to include Mr. Abdulmutallab in a watch-list is part of the

overall system failure", and then recommended that we "Accelerate information technology enhancements, to include knowledge discovery, database integration, cross-database searches, and the ability to correlate biographic information with terrorism-related intelligence".

Does our technology today enable us to assess every single passenger's risk profile, in order to determine his specific risk level and to immediately communicate that information to other agencies for extra screening or follow up?

Response:

Neither the TSC nor the FBI develops risk profiles for passengers. The Department of Homeland Security (DHS) may have further information regarding risk profiling technology for passenger screening.

Questions Posed by Senator Feingold

8. The President has directed the FBI to review the watch list nomination process and make possible recommendations.

a. What is the status of that review?

Response:

Following the attempted Christmas day terrorist attack, the President directed a review of the circumstances that permitted Umar Farouk Abdulmutallab to board Northwest Airlines Flight 253. Following this review, the President concluded that action must be taken to ensure that the standards, practices, and business processes that have been in place since the 9/11/01 attacks are appropriately robust to address the current terrorist threat and the evolving threat that will face our nation in the coming years. As a result, the TSC was given two instructions. First, the TSC was tasked to conduct a thorough review of the TSDB to ascertain the current visa status of all known and suspected terrorists, beginning with the No Fly List. That review has been completed. Second, the TSC was asked to develop recommendations on whether adjustments should be made to the watchlisting nomination criteria, including the biographic and derogatory criteria for inclusion in the Terrorist Identities Datamart Environment (TIDE), the TSDB, the No Fly list, and the Selectee list. To develop these recommendations, the TSC convened its Policy Board Working Group (PBWG), which includes representatives from the Central Intelligence Agency (CIA), National Security Agency (NSA), U.S. Department of Defense (DoD), U.S. Department of State (DOS), NCTC, NSC, DOJ, and DHS to achieve interagency consensus. The TSC will work with the PBWG to develop appropriate recommendations to be forwarded to the President for consideration.

b. As part of that review, what steps are you considering to ensure innocent Americans are not mistakenly identified as being on the watch list?

Response:

The concern arising out of the attempted Christmas day attack was that some people who should be prohibited from boarding aircraft were permitted to do so because they were not included on the appropriate watchlist. To prevent future such attacks, a threat-related target group was identified and individuals from specific high-threat countries who were already included in TIDE or TSDB were added to the No Fly and Selectee lists.

To ensure that innocent Americans are not mistakenly among these individuals, TSC is working with the NCTC and others to conduct a comprehensive review of the derogatory information associated with the names on the list. In addition, in 2007 DHS launched its Traveler Redress Inquiry Program (TRIP) as the central gateway for redress complaints addressed to DHS agencies. DHS TRIP is a Web-based program that can be accessed through the DHS website at www.dhs.gov/trip. If a traveler believes he or she has been delayed or inconvenienced during screening due to watchlist status, that traveler is encouraged to submit a redress complaint thorough DHS TRIP.

TSC has also established a process for assisting those who are subjected to additional security scrutiny. In 2008, TSC initiated a proactive Terrorist Encounter Review Process (TERP) to analyze and review the TSDB records of watchlisted individuals who are frequently encountered by the U.S. Government. Under TERP, TSC reviews TSDB records to ensure that frequently encountered individuals warrant continued placement on the terrorist watchlist. TSC also examines these records to ensure they contain current and accurate information and to determine whether any additional information could be included in the records to reduce instances of misidentification.

9. The FBI's internal review on Fort Hood called for "strengthened training addressing legal restrictions which govern the retention and dissemination of information." Press reports indicate that the Joint Terrorism Task Force that examined Major Hasan's case prior to the attack at Fort Hood shared information on Hasan with DOD personnel. Is that accurate? Did the FBI find that there were any legal barriers to sharing information about Major Hasan that was in its possession with the Department of Defense?

Response:

There are legal restrictions on the FBI's ability to share sensitive information, including those imposed by the Foreign Intelligence Surveillance Act (FISA), Attorney General's Guidelines, and Executive Order 12333, and those that apply to the dissemination of classified information. Generally, information about U.S. persons from sensitive sources cannot be disclosed unless certain legal thresholds

are met. Nonetheless, under the Memorandum of Understanding governing DoD participation on FBI-led JTTFs, DoD detailees to the JTTFs may share information outside of the JTTFs with permission from an FBI supervisor.

DoD agents assigned to a JTTF took part in evaluating certain information regarding Major Hasan that came to the FBI's attention prior to the shootings. Because they believed the information was explainable by Major Hasan's academic research and because there was no derogatory information in the personnel files they reviewed, they determined, in consultation with an FBI JTTF supervisor, that Major Hasan was not involved in terrorist activity or planning. Based on that judgment, a decision was made not to contact Major Hasan's superiors in the Army.

Questions Posed by Senator Specter

10. In addition to the many efforts you discussed at the hearing, are there any changes that you would suggest other agencies implement to increase security?

Response:

The FBI works closely with its many Federal law enforcement and intelligence community partners at both operational and managerial levels to improve our national security, and we will continue to communicate directly with those agencies on these matters of joint concern.

11. You mentioned in your testimony that home-grown terrorists and "lone wolf" attacks are serious threats in addition to terrorists acting with external support. Should security check-points for domestic flights adopt the enhanced screening standards applied to international travelers?

Response:

The FBI defers to DHS' Transportation Security Administration as to the screening standards most appropriate for both domestic and international travelers.

Questions Posed by Senator Sessions

12. During your testimony before the Committee, you were asked about how the decisions regarding Umar Farouk Abdulmutallab's questioning on December 25th were made.

a. At the time of the attempted bombing attack on Christmas Day 2009, was there a policy, protocol or any written guidance in place on how the U.S. government would

handle the detention and questioning of U.S. persons or non-U.S. persons apprehended in the United States who have attempted or committed a terrorist attack or for whom the Government has cause to believe that they are engaged in terrorist activities?

b. Is there now such a policy, protocol or any written guidance in place?

c. If such guidance existed or now exists, please provide a copy to the Committee, enclosing it in a classified annex if necessary.

Response to subparts a through c:

Homeland Security Presidential Directive (HSPD) 5, signed in 2003 by President Bush, assigns to the Attorney General the lead responsibility for investigating terrorist acts committed within the United States. Consistent with that responsibility, the FBI responded to the scene and took custody of the suspect. There are a number of laws and rules that govern what must occur when a suspect is arrested without an arrest warrant. First and foremost, the U.S. Supreme Court has held that the Fourth Amendment requires that the facts justifying the arrest be presented to a court "promptly." Moreover, Rule 5 of the Federal Rules of Criminal Procedure requires that the defendant be taken before a judicial officer "without unnecessary delay," at which time the court will advise the defendant of his rights. HSPD-5 has previously been provided to the Committee.

Questions Posed by Senator Hatch

13. There are three expiring provisions of the PATRIOT Act. In previous testimony before this committee, you have heralded these provisions as critical investigative tools that the FBI needs to detect and thwart terror plots. For example, the three separate terror plots in Illinois, Texas and New York detected by the FBI last September. In December, Congress only temporarily reauthorized these provisions without any modifications. I have some concerns that any modifications to these investigative tools would "water them down" and unnecessarily increase the investigative burden on the FBI before these tools may be used.

a. Can you tell me if you would support a full reauthorization of these provisions without any modifications?

Response:

The response to this inquiry is being provided separately.

b. Can you confirm if any of these expiring provisions were used by the FBI in the investigation of these plots?

Response:

The FBI continues to support the renewal of the three expiring provisions.

Additional information responsive to this inquiry is classified and is, therefore, provided separately.

14. With regard to the decision to arrest of Umar Farouk Abdulmutallab on federal charges for his attempted bombing of NW 253. During the hearing, you informed the committee that the suspect was interviewed before any Miranda warnings were given. The administration asserts that the suspect provided valuable information during this 90 minute interview.

a. What if any guidance has FBI headquarters communicated field offices or JTTFs by either electronic communication, policy directives or standard operating procedures as to how possible terrorists in custody are to be held, detained and interviewed?

Response:

FBI guidance regarding arrest and interview procedures is conveyed to Special Agents primarily through New Agent and subsequent training and the FBI Legal Handbook for Special Agents (for example, section 7-3 of that handbook concerns custodial interviews). As that training and written guidance make clear, investigations related to Federal criminal violations and/or threats to the national security must be conducted in a manner consistent with the laws, regulations, national security directives, policies, and guidelines governing the circumstances involved, and each case must be handled in accordance with its unique facts and circumstances. Investigative subjects vary widely in terms of motivation, level of commitment, intelligence, and dozens of other factors. An investigative technique that may work well in one case may not work at all in another case. Although the FBI ensures that all FBI investigators and their supervisors understand that the FBI's first priority is the prevention of terrorist attacks, the FBI allows these agents and their supervisors to exercise considerable discretion in the handling of each case.

b. If the policy was changed, what was the previous policy and when did it change?

Response:

This policy has not changed.

c. Has it been communicated to FBI offices and task forces that agents will operate under the assumption that potential terrorism cases will be referred to the U.S. Attorney's office for prosecution?

Response:

Pursuant to HSPD-5, the Attorney General has lead responsibility for any terrorism act committed within the United States. Consistent with that responsibility, the FBI will respond to the scene of any such attempted terrorist attack and will conduct an appropriate investigation in compliance with the Attorney General's Guidelines for Domestic FBI Operations. The FBI has no legal authority to proceed against a terrorism suspect who is arrested within the United States in any venue other than an Article III court. There have been only two instances since 2001 in which civilians arrested within the United States were placed in military custody for some period of time. In both instances, the individuals were initially taken into custody and detained by Federal law enforcement officials. The transfers from law enforcement to military custody occurred by order of the Commander in Chief, and the civilians were later returned to Article III courts for disposition of their cases.

d. Are potential terrorist[s] expeditiously presented to the High Value Detainee Interrogation Group for possible follow up or additional action before the suspect is arrested and adjudicated in federal court?

Response:

The High Value Detainee Interrogation Group (HIG) was designed to ensure the availability of interagency interrogation teams, called Mobile Interrogation Teams (MITs), to interrogate high-value detainees. These interagency MITs train together against targeted individuals with a view toward deploying the MIT if and when its target is captured. In appropriate circumstances, a MIT may be deployed to interrogate a high-value detainee who is believed to be of significant intelligence value, even if he was not being actively targeted before his arrest or capture.

e. Was the information provided by the suspect immediately reviewed or corroborated with other government entities like the High Value Detainee Interrogation Group, NCTC or other assets to determine if the suspect was truthful in his responses to questions pre-Miranda?

Response:

Entities such as NCTC are involved in analysis and production of intelligence. NCTC's analysis may be used by the investigating agents and other interviewers - and, if a MIT were deployed, by the MIT - in consultation with subject matter experts to help inform the questioning and evaluate whether a subject is being truthful.

In this case the information obtained during the un-Mirandized interview was shared promptly with the USIC.

15. The Terrorist Screening Center (TSC) is responsible for generating terrorist screening databases, look out records and watch lists to front line screening agencies and state and local law enforcement. These alerts and lookouts are made available to state and local agencies through NCIC's Violent Gang and Terrorist Offender File. In last September's case of alleged Texas terror plot bomber, Hosam Smadi, the system worked and a Deputy Sheriff was informed that Smadi was under investigation by the FBI during a routine traffic stop. However, when Smadi was run through NCIC there was no information in his alert regarding his visa overstay.

a. Can you tell me if during the course of its investigation, the FBI had received information from either DHS or the State Department regarding the immigration or visa status of Hosan Smadi?

Response:

The FBI's Dallas Division learned of Smadi's immigration status through the Immigration and Customs Enforcement (ICE) agent working on the FBI's North Texas JTTF. Through the collaboration opportunity afforded by the JTTF, the FBI and ICE were able to quickly determine Smadi's immigration/visa status.

b. Does FBI obtain information from either State or DHS regarding the visa status of persons under investigation for terrorism or other criminal violations?

Response:

Yes. The FBI regularly obtains visa information concerning persons under investigation for terrorism and other criminal violations. Both ICE and DOS are typically represented on the FBI's JTTFs.

Questions Posed by Senator Grassley

16 According to recent congressional testimony provided by Mr. Timothy Healy, Director of the Terrorist Screening Center (TSC) administered by the FBI, a person nominated to be on the Terrorist Watchlist must meet two principal requirements: 1) the biographic information associated with the individual must contain sufficient identifying data so the person can be matched to the watch list; and 2) the facts and circumstances linking the watch list nominee must meet the "reasonable suspicion" standard of review. Mr. Healy stated, "Mere guesses or inarticulable 'hunches' are not enough to constitute reasonable suspicion."

a. Standing alone, does the report from the father in this case meet the "reasonable suspicion" standard in your view?

b. The State Department and DHS have indicated in their briefings that the information from the father would not, by itself, have been enough to place Abdulmutallab

on the TSC watch list because of a particular policy which prevents listing an individual based solely on information from a single source - regardless of how credible or reliable the source may be. Is that an accurate description of the policy, and if so, why should a single reliable source not be enough to place a foreign national on the watchlist?

Response to subparts a and b:

The report indicated that the father was concerned that his son *may be* associating with extremists. Because the "reasonable suspicion" implementation guidance in effect at the time did not permit watchlisting based solely on uncorroborated statements from "walk-ins," some additional corroboration would have been needed to place Abdulmutallab on the watchlist. The TSC's interagency Policy Board Working Group (PBWG) is reviewing the guidance pertaining to source verification and report corroboration to determine whether that guidance should be revised.

c. Given that al-Qaeda has extensively recruited non-U.S. citizens to carry out its attacks, has the TSC considered revising its nomination standards to allow a less restrictive standard of review for the listing of non-U.S. persons suspected of terrorism on the no fly list?

Response:

The President has directed the TSC to recommend whether changes to the watchlisting criteria and implementation guidance are required, and this process is underway. To develop recommendations responsive to the President's directive, the TSC convened its interagency PBWG, on which the NSC, DOS, DOJ, NCTC, DHS, CIA, NSA, and DoD are represented.

**Responses of the Federal Bureau of Investigation
to Questions for the Record
Arising from the January 20, 2010, Hearing Before the
Senate Committee on the Judiciary
Regarding "Securing America's Safety: Improving the Effectiveness of
Anti-Terrorism Tools and Inter-Agency Communication"**

Questions Posed by Senator Hatch

13. There are three expiring provisions of the PATRIOT Act. In previous testimony before this committee, you have heralded these provisions as critical investigative tools that the FBI needs to detect and thwart terror plots. For example, the three separate terror plots in Illinois, Texas and New York detected by the FBI last September. In December, Congress only temporarily reauthorized these provisions without any modifications. I have some concerns that any modifications to these investigative tools would "water them down" and unnecessarily increase the investigative burden on the FBI before these tools may be used.

a. Can you tell me if you would support a full reauthorization of these provisions without any modifications?

Response:

The FBI continues to support the reauthorization of the USA PATRIOT Act's expiring provisions, which concern roving wiretaps, Section 215 business record orders, and the "lone wolf" provision. The Attorney General and Director of National Intelligence have previously advised the Congress that S. 1692, the USA PATRIOT Act Sunset Extension Act, as reported by the Senate Judiciary Committee, strikes the right balance by both reauthorizing these essential national security tools and enhancing statutory protections for civil liberties and privacy in the exercise of these and related authorities. Since the bill was reported, a number of specific changes have been negotiated with the sponsors of the bill for inclusion in the final version of this legislation. Among these are several provisions derived from the bills reported by the House Judiciary Committee and introduced by House Permanent Select Committee on Intelligence Chairman Silvestre Reyes in November.

The FBI has been authorized to use the roving wiretap authority many times and we have found that it increases efficiency in critical investigations. This authority affords us an important intelligence gathering tool in a small, but significant, subset of electronic surveillance orders issued under FISA. Roving wiretap authority is particularly critical for effective surveillance of investigative subjects who have received training in countersurveillance methods.

Section 215 orders for business records play an important role in national security investigations as well. This authority allows us to obtain records in national security investigations that cannot be obtained through the use of National Security Letters. In practice, this tool is typically no more intrusive than a grand jury subpoena in a criminal case. Unlike most criminal cases, though, the operational secrecy requirements of most intelligence investigations require the secrecy afforded by this FISA authority. There will continue to be instances in which FBI agents must obtain information that does not fall within the scope of National Security Letter authorities and is needed in an operating environment that precludes the use of less secure criminal investigative authorities.

Finally, although the "lone wolf" provision has never been used, it is an important investigative option that must remain available. This provision gives the FBI the flexibility to obtain FISA warrants and orders in the rare circumstances in which a non-U.S. person engages in terrorist activities, but his or her nexus to a known terrorist group is unknown.

b. Can you confirm if any of these expiring provisions were used by the FBI in the investigation of these plots?

Response:

As discussed previously, the FBI continues to support the renewal of the three expiring provisions.

Additional information responsive to this inquiry is classified and is, therefore, provided separately.