U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

July 28, 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 Robert Mueller, Director of the Federal Bureau of Investigation, 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." Please note that the attached document includes a response to question 13(a) and therefore represents a complete response to the unclassified questions. 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 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.

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.