Counterterrorism Information Sharing With Other Federal Agencies and with State and Local Governments and the Private Sector

Eleanor Hill, Staff Director, Joint Inquiry Staff

October 1, 2002

INTRODUCTION

Mr. Chairman and members of the Joint Committee, good morning. In prior hearings, we have discussed specific information sharing issues relating to the performance of the Intelligence Community prior to the events of September 11. Today, I will discuss what our review has uncovered regarding the more systemic aspects of information sharing between the agencies of the Intelligence Community, and between those agencies and other federal, state, and local entities. Before addressing the issue of information sharing, I would, however, like to summarize our review of what the non-Intelligence Community agencies knew about the hijackers.

The Hijackers

We have not found any evidence that non-Intelligence Community agencies had any information prior to September 11 that the 19 individuals who took part in the September 11 attacks had terrorist ties. We also found that the non-Intelligence Community agencies were focused on specific threats to their areas of responsibility, such as airline hijackings or an individual terrorist crossing the border. We did not find any significant focus on a "war" against Bin Ladin, in which terrorist operatives might launch multiple attacks against the continental United States using airplanes as weapons. While the FAA, Customs, State, and INS each had data concerning the 19 hijackers, that data was not related to their terrorist activities or associations. As a result, none of this information would, by itself, have aroused suspicions regarding a planned terrorist attack within the United States. Instead, these agencies had routine information concerning the vital statistics, travel, immigration, and medical status of some of the hijackers.

Prior to September 11th, the FAA had airman records on hijackers Marwan Alshehhi, Mohamed Atta, Hani Hanjour, and Ziad Jarrah. Mohamed Atta filled out a medical history form on July 24, 2000. Marwan Alshehhi was issued a medical certificate on July 24, 2000. A medical record concerning Hani Hanjour dated back to 1996, while a medical record for Ziad Jarrah was issued on July 11, 2000. While the

FAA had some records relating to Zacarias Moussaoui, it could not find any evidence that Moussaoui was ever issued a recreational pilot or higher-level airman certificate.

The INS also had records concerning the 19 hijackers—specifically the type of visa and the duration of the stay adjudicated by the immigration officer for each individual. INS records show that three of the 19, Satam Al Suqami, Nawaf Al Hazmi, and Hani Hanjour had overstayed their visas. According to the INS, Mohamed Atta filed an application to change his visa status from B-1 to M-1, and this was granted on July 17, 2001. The B-1 visa is issued to foreign nationals for personal travel to the United States while the M-1 visa is issued to foreign nationals to study in the United States. However, on July 19, 2001, Mr. Atta was admitted to the United States based on his then current B-1 visitor visa.

U.S. Customs Service officials advised the staff that the only information Customs had concerning the 19 hijackers prior to September 11 was contained in the routine forms they filled out when they arrived in the United States.

Information Sharing Obstacles to Counterterrorism

The Joint Inquiry Staff interviewed numerous Intelligence Community officials and officials of departments and agencies outside the Intelligence Community to determine the extent to which terrorist-related information flows as necessary to avert terrorist attacks. The staff also reviewed relevant documents at the Departments of State, Treasury, Defense, Transportation, and Energy and at the U.S. Customs Service and the Immigration and Naturalization Service (INS), focusing on information received from the Intelligence Community.

Our review also included what the agencies outside the Intelligence Community knew about the hijackers before September 11 and the specific information on which that knowledge was based. The staff reviewed visa and immigration information, and also what had been shared with these agencies regarding threats to U.S. landmarks using aircraft as weapons, and terrorist financing in the United States. The staff also interviewed various officials in Department Of Defense agencies and components, and in the military services, regarding the support they provided to or received from, the Intelligence Community agencies.

In February 2001, Director of Central Intelligence (DCI) George Tenet publicly testified to Congress that "the threat from terrorism is real, it is immediate, and it is evolving." Furthermore, "[Osama] bin Ladin and his global network of lieutenants and associates remain the most immediate and serious threat." The events of September 11, 2001, in retrospect, underscore the significance of the DCI's concerns. Our work to date indicates that the flow of information between all agencies did not necessarily keep pace with the increasing nature of the threat.

During the course of our interviews, intelligence and non-intelligence personnel alike complain that a range of political, cultural, jurisdictional, legal, and bureaucratic issues are ever-present hurdles to information sharing. Prior to the passage of the USA Patriot Act, many suggested that law enforcement information was not adequately shared with the Intelligence Community. The reverse was also apparently true despite amendments to the National Security Act in the 1990s designed to make clear that foreign intelligence could be collected for, and shared with, U.S. law enforcement agencies.

We were also told that not all threat information in possession of the Intelligence Community or law enforcement agencies is shared with agencies that need it the most in order to counter the threats. For example, the FAA was not provided a copy of the FBI's Phoenix memorandum prior to September 11, 2001 and still did not have a copy two weeks after the matter had become public in early 2002. In another example, the CIA did not provide the Department of State with a large number of intelligence reports that included the names of terrorist suspects until shortly after September 11, 2001. The reasons for this reluctance to share range from a legitimate concern about the protection of intelligence sources and methods to a lack of understanding of the functions of other agencies.

The vast majority of the information related to the hijackers or to threats posed by aircraft came to the non-Intelligence Community agencies from the CIA, NSA, and FBI. According to officials from the Departments of Transportation, State, Energy, Defense, and Treasury, unless information in the possession of the CIA, NSA, and FBI is shared on a timely basis, they are unable to include dangerous individuals on various watch lists to either deny them entry into the United States or apprehend suspected terrorists in the United States. The State Department, the Immigration and Naturalization Service (INS) and the U.S. Customs Service all maintain watchlists of named individuals. The Federal Aviation Administration (FAA), Drug Enforcement Administration (DEA), INS, and other agencies also perform a limited amount of information collection designed to place individuals on watchlists.

The staff review, to date, has found no single agency or database or computer network that integrates all counter terrorism information nationwide. Information about the hijackers and al-Qa'ida can be found in disparate databases spread among a range of intelligence and civilian agencies. Specifically, as exemplified by the Phoenix communication that was discussed in detail at a prior hearing, FBI information related to possible al-Qa'ida terrorists was scattered in various regional offices and not shared with the FBI headquarters or other agencies. Furthermore, law enforcement, immigration, visa, and intelligence information related to the 19 hijackers was not organized in any manner to allow for any one agency to detect terrorism-related trends and patterns in their activities.

Numerous officials state that there are many hurdles to sharing information. A major issue relates to the availability of properly cleared personnel. Federal officials told us that clearing a person for access to Sensitive Compartmented Intelligence (SCI) takes anywhere from one year to a year and a half and describe the process as cumbersome and unwieldy. However, without SCI clearances, non-intelligence community agencies are often unable to access vital counterterrorism-related information. Some federal agencies we visited which did not have personnel cleared for SCI data, advised that they could have benefited from receiving more specific data on potential terrorists. We were also told that many state and local agencies do not have personnel cleared for even the lowest level of access to national security information, let alone SCI access. As a result, while appropriately cleared FAA, TSA, INS, and Department of State officials may receive significant intelligence information, they may be unable to disseminate data within their organization or to state and local officials because the potential recipients are not cleared to receive it.

Another difficulty mentioned repeatedly is the "originator control" or ORCON caveat. Agencies that generate intelligence impose this caveat when disseminating raw and finished intelligence to prohibit further dissemination without their approval. Thus, an agency may receive very important information that could be of use to a third agency that is not a recipient, but may be unable to share it because of the caveat. Although this matter can be resolved through agreed-upon procedures, the process can be lengthy and cumbersome and may not meet the near-real time lines often required to track and apprehend terrorist suspects.

We were told that because information sharing is inconsistent and haphazard, agencies have tried various means available to them to circumvent the hurdles. These include: (1) signed memoranda of agreements with other agencies, (2) the use of detailed employees to other intelligence and law enforcement agencies; (3) participation in joint task forces; and (4) attempts to design and field common databases.

Agencies Detail Employees Try To Ensure Access To Intelligence Information

One method of dealing with information sharing issues is for agencies to detail employees to CIA, NSA, FBI, and other agencies in an attempt to improve access to relevant information on a timely basis. Theoretically, at least, the agencies believe this is one of the most effective ways to access a greater amount of information from the Intelligence Community. Thus, the Departments of State, Transportation, Treasury, and Energy and the INS, Customs, and other organizations have utilized detailees at the DCI's Counterterrorist Center (CTC), at the FBI, and, to a lesser extent, at the NSA. In turn, Intelligence Community agencies also send detailees to the non-intelligence agencies and law enforcement agencies. Numerous task forces and cooperative agreements exist between the DOJ's FBI and border security and intelligence agencies.

Although sending employees to another agency has merits, it is an imperfect response to the problem. The JIS was told repeatedly that detailees are not afforded the same access to information as host agency employees. The almost unanimous opinion among the detailing agencies is that host agencies still restrict access to information and limit the databases that can be queried by detailees from other agencies on grounds of personnel or information security, and intelligence policies. We were told that detailees are often advised about the existence of intelligence after an ad hoc judgment to share the information is made by host agency employees. Representatives of the detailing agencies advised that host agency employees may not have the proper understanding of the issues that are of interest to other agencies and consequently provide detailees with information that often lacks proper context. Representatives of the detailing agencies also suggested that success in gaining access to information can be personality driven. All agencies recognized that agency to agency open and secure access through electronic means would be the optimal solution answer whereas the detailing of employees is basically a value-added approach.

Joint Terrorism Task Forces

To improve information sharing, the DOJ, through the FBI, has established 56 Joint Terrorism Task Forces (JTTFs) to involve other federal, state, and local agencies in investigation of terrorist events. The JTTF program is intended to prevent acts of terrorism before they occur by assisting in identification, investigations, and prosecution. Each JTTF is responsible for dealing with domestic and international terrorism matters within the jurisdiction of the local FBI field office. Agencies participating in the JTTF are required to enter a formal memorandum of understanding that identifies the objectives of the JTTF as both reactive and proactive. In its reactive mission, the JTTF responds to and investigates terrorist incidents. In its proactive mission, the JTTF investigates domestic and foreign terrorist groups and individuals targeting or operating within its jurisdiction with the goal of preventing terrorist events.

The JTTFs are described as an important force multiplier for an FBI field office. The personnel who work at a JTTF serve as, and are treated like, FBI special agents. They are given cases to investigate and access to most of the field office's information systems. In the New York field office, however, JTTF personnel told the staff that non-FBI personnel are prevented in some cases from having access to the FBI's information systems. The result is that non-FBI members must rely on FBI special agents to obtain information that will assist them in their investigations.

The non-FBI members' knowledge, experience and affiliations with state and local law enforcement organizations serve to enhance the ability of the JTTF to deal with terrorism. In this regard, we were told the most highly lauded member of the JTTF is often the INS. INS membership in the JTTF repeatedly has allowed the FBI personnel in the New York, Boston, and Phoenix field offices to use violations of the immigration laws to disrupt and obtain information from individuals the FBI suspects of being terrorists or of having terrorist connections. The INS-FBI collaboration has been instrumental in getting relevant information from these individuals.

The staff was told that, a consistent complaint against the JTTF program has been the lack of participation by local law enforcement organizations. While these organizations are often viewed as not being interested in participating in the JTTF, their absence leaves a void in the JTTF. For their part, local law enforcement organizations assert that by participating in the JTTF program they lose officers, to work on what are largely considered " FBI issues", who would otherwise be patrolling their cities' neighborhoods. Another complaint from JTTF participants is that, prior to September 11th, individuals who were assigned to the JTTF were not always the best for the job. We were told that some law enforcement organizations reportedly viewed the JTTF as a way of getting rid of "deadwood and working retired." This trend changed dramatically after September 11th, we are told.

FAA/TSA

Following the hijacking of a TWA aircraft in the Middle East in the mid 1980s the FAA established a small office (now a part of the Transportation Security Administration) to review the incoming intelligence regarding threats to aviation. The intelligence is translated into information circulars, emergency amendments and security directives for the aviation industry. The circulars and directives are issued to domestic and foreign airlines and to the airports to advise them of current and potential terrorist threats. They are also provided to the Intelligence Community and law enforcement agencies.

Prior to September 11, the FAA had issued a number of circulars and directives as a direct result of intelligence received from the Intelligence Community regarding extremist Islamic groups. These FAA publications advised the airlines of the methods that might be used by such groups to hijack an airplane or to plant explosives in airplanes. None, however, have been found that discussed crashing planes into buildings.

The Intelligence Community is required by law to provide the Department of Transportation (DOT) with intelligence concerning international terrorism. As a result, the Department receives intelligence from the CIA, the Department of State, FBI, NSA, and DIA. However, DOT officials advise the staff that they do not believe they receive all the available intelligence that is needed to perform their mission. In their view, the agencies that collect the information make decisions on what is relevant for, and what should be shared with, the DOT. The issue reportedly is one of context and depth of understanding. By not receiving the sum total of the intelligence on all transportation issues, the TSA may not be able to connect events or to link suspicious activities. Finally, TSA officials stated that, although they can submit their requirements to the Intelligence Community through established procedures, there is nothing that requires the Intelligence Community to collect against those requirements.

Although no indications have been found that the FAA knew of the terrorist connections of the hijackers, the FAA did have detailed information regarding those who were pilots. The FAA maintains records of all certificated airman—those who possess a U.S.-issued certificate, and also on all U.S. registered aircraft. According to the FAA, there are over one million airmen files, of which approximately 626,000 are pilots. Representatives of the FAA stated that the airmen file remains open until receipt of a death certificate. Each certificate contains specific medical information, flight test results, score, engine ratings, incident history, and enforcement activity. These records are kept in Oklahoma City, Oklahoma by the Department of Transportation—specifically the FAA Civil Aviation Registry—and are available to all federal, state and local law enforcement agencies.

According to TSA, shortly after Zacarias Moussaoui's arrest, the FBI contacted it and asked for information on him from the airman records. FAA personnel in Minneapolis advised the FBI to contact the FAA office in Chicago and that office put the FBI in touch with the Oklahoma City center. TSA officials in Washington, D.C. told the staff that they were puzzled that the FBI did not contact the Oklahoma center directly since it was designed to support law enforcement.

Immigration and Naturalization Service

The Immigration and Naturalization Service (INS) maintains records on all visitors who arrive in the United States. INS officials told the staff that the Law Enforcement Support Center (LESC) in Burlington, Vermont is a key data-sharing center designed to support other law enforcement agencies. The LESC assists in determining the status of detainees or to find persons. INS officials stated that the August 2001 notice to watchlist Nawaf al Hazmi and Kahlid al Mihdhar was not accompanied by any specific notation that indicated that the INS should use all means possible to find these two suspects. INS officials said that, had they been told to put the highest priority on that search, they would have used the LESC and might have found the two suspects prior to September 11, 2001.

Defense Intelligence Agency

The Director of DIA chairs a standing committee that serves as an integrating mechanisms for the DOD: the Military Intelligence Board (MIB). DCI representatives usually attend and participate in its discussions. Over time, the MIB has wrestled with information sharing issues prior to September 11. According to the DIA, information-sharing issues such as restrictive caveats (e.g., originator or "ORCON" controlled information), handling of information in virtual and collaborative workspaces, limited distribution to senior officials only, and support to homeland defense have been discussed by the MIB since at least the mid-1990's. While most of the specific discussion at MIB meetings is classified, there are enough unclassified examples to provide some definition of the range of information sharing topics addressed. For example, the need to establish an information sharing mechanism was addressed at least as early as February 1995 in the context of multi-agency operations in Haiti. Several additional examples follow, drawn from the records of the proceedings of the group.

In September 1998, an MIB was convened to receive briefings on the East African Embassy Bombings and the War on Terrorism. Generally recognizing the need for broad sharing of information in that context, one Command representative observed that there must be a "domestic piece", referring to FBI reporting. Another representative stressed that there was a "commercial piece" as well, with the FAA. Yet a third representative encouraged intra-organizational information sharing as it had done within its organization. Finally, another Command supported breaking through the existing information restriction barriers and recommended a collaborative strategy regarding how to examine and attack terrorist organizations. It is not clear whether any follow-up actions were taken as a result of this discussion.

In April 1999, the MIB met to receive a briefing on computer network defense. Challenges to both network defense and information sharing were listed as: law enforcement vs. public interests; the interagency process; and policy and legal issues

In January 2000, the MIB met for a briefing concerning a DIA asymmetric warfare initiative. Both the NSA and the Coast Guard representatives spoke to the legal complications of the portion of the concept that pertained to homeland defense. During a July 2000 update, NSA reiterated its concern about policy and legal issues, especially regarding NSA collection in support of homeland defense and terrorism. The Coast Guard cautioned that new environments and new threats might mean old rules could no longer apply. Again it is not yet apparent whether this discussion of obstacles to real information sharing needs led to further action.

In October 2000, the MIB discussed the issue of "need to know." A DCI Community Management staff representative said the CIA was working to resolve the issue in connection with information architectures that would allow analysts to share information. A DIA attendee said that philosophically, defense intelligence had moved away from "need to know," but that CIA still adhered to the principle "as a foundation." The DIA attendee concluded that the defense intelligence community would not be able to bridge the gap with CIA on this information sharing issue.

Senior DIA officials told the staff that information-sharing issues are not new to the Intelligence Community and are not limited to the context of September 11. According to them, the basic legal, community, cultural, and technological barriers have been understood for years. After the USS Cole attack, the DIA reportedly took significant steps to alter its structure, processes, products, and policies associated with terrorism analysis. DIA officials advised that the DIA now challenges its analysts to "think out of the box" and exploit all relevant information, including open source reporting. They also stated that DIA has implemented mechanisms that allow more effective receipt and dissemination of critical intelligence information.

The DIA has established a Joint Intelligence Task Force for Combating Terrorism (JITF-CT) to help enhance terrorist threat warning and analysis capabilities and significantly enhance communications and sharing between DIA, the FBI, and CIA. Deputy Secretary of Defense Paul Wolfowitz identified the value of the JITF-CT during his testimony to the Joint Inquiry on September 19, 2002. He also identified the issue of information discovery where "many agencies collect intelligence and lots of agencies analyze intelligence, but no one is responsible for the bridge between collection and analysis." Finally, Mr. Wolfowitz questioned the current culture that discourages collaboration and criticized the lack of sharing of information that leads to forfeiting of U.S. technological advantages.

According to DIA personnel, there have been mixed results with these Intelligence Community partnerships, i.e., the mere act of assigning an analyst to another organization does not ensure a greater level of access to information or more open sharing of information. DIA acknowledged that its analysts who are detailed to counterpart organizations do not have unfettered and unconditional access to all relevant terrorist information. Former DIA Director Admiral Thomas Wilson explained to the staff that "information sharing" implies that one "owns the information." He did not agree with that concept. According to Wilson, agencies need to change their culture and shed the belief that they own the information—the information belongs to the United States Government and the entire Intelligence Community.

Department of Treasury

Several Treasury Department components receive intelligence relating to financial matters from the CIA, NSA, FBI and other intelligence agencies. The JIS interviewed Treasury officials at the Financial Crimes Enforcement Network (FinCEN), the Office of the Financial Assets Control (OFAC), the Secret Service, and US Customs.

Officials in Treasury's Financial Crimes Enforcement Network (FinCEN) and the U.S. Customs Service reported to the staff that they submit intelligence requirements to the Intelligence Community, but have no assurances that the intelligence will be collected and provided to them on a timely and regular basis.

The Secret Service at Treasury occupies a unique position because of its primary mission to protect the President of the United States. According to the Secret Service, it receives the intelligence that is necessary for it to perform that particular mission. It also reportedly receives all relevant intelligence regarding the maintenance of the protective perimeter around the White House.

Post-September 11, U.S. Customs officials used information available in Treasury databases to develop a comprehensive analysis of the travel, finances, and linkages of the hijackers. Specifically, U.S. Customs Service analysts used Suspicious Activity Reports (SARs), Currency or Monetary Instrument Reports (CMIRs), and Current Transaction Reports (CTRs) obtained from the Treasury Department. Much of the analysis was completed by November 2001.

Customs officials advised that the majority of the information used in that analysis to show the domestic and international activities and associations of the hijackers came from law enforcement databases—specifically the Inter-agency Border Inspection System (IBIS)—and not intelligence. IBIS is a major information-sharing system that connects Customs with INS, the Department of State, FBI, National Law Enforcement

Telecommunications System (NLETS), Drug Enforcement Agency (DEA), Alcohol, Tobacco, and Firearms (ATF), Secret Service, Internal Revenue Service (IRS), FAA, and the Royal Canadian Mounted Police. According to the Customs service, there are over 30,000 users of IBIS, but it has no connection to the Intelligence Community. Customs officials told the staff that they need to have regular and consistent information from the Intelligence Community on terrorism related matters.

Department Of State

As mentioned earlier, and explained in more detail in the September 18, 2002 JIS staff statement, State Department officials advised the staff that at least 1,500 CIA Central Intelligence Reports (CIRs) containing terrorist names were not provided to the TIPOFF watchlisting program until after September 11, 2001. After an analysis of those CIRs was completed, the names of approximately 150 suspected terrorists were identified and 58 new suspected terrorist names were added to the TIPOFF watchlist. This lapse in sharing intelligence, and the failure to add the names of at least two of the hijackers to the State watchlist prior to September 11, were attributed to a lack both of resources and of awareness of watchlisting. State Department officials advised that they have had continuing difficulty obtaining data for watchlisting purposes from the National Crime Information Center's Interstate Identification Index (NCIC III) that is managed by the FBI.

Foreign Terrorist Tracking Task Force

The Attorney General established the Foreign Terrorist Tracking Task Force (FTTTF) in October 2001 at the request of the President. The FTTTF's mission is to assist in keeping foreign terrorists and their supporters out of the United States by developing information through "data-mining" technologies and providing that information to law enforcement and other operational agencies. The FTTTF relies on public, government, and other databases to link relevant information about terrorists and their supporters.

According to FTTTF officials, it is attempting to solve the problem of identifying possible terrorist suspects. The FTTTF is intended to co-locate data from the law enforcement and intelligence communities, and other government and non-government sources and, then, provide that information to federal, state, and local operational agencies.

FTTTF officials state that they are encouraged that the databases and interagency participation in the program have been progressing as envisioned. The FTTTF is not a separate agency, it is a multi-agency task force that is entirely staffed with detailees from different agencies. The Department of Defense's Joint Counterintelligence Assessment Group provides primary technical support to FTTTF.

FTTTF officials reported that several thousand individuals from several countries have been already identified as "abscondees" within the United States by the FTTTF. Many new addresses for "cold" abscondees were provided to the INS and the INS is now working closely with the FTTTF to identify individuals who are engaged in immigration law violations. Additionally, the FTTTF works closely with the FBI on the identification and location of terrorists and their supporters.

Executive And Congressional Recognition Of Information Sharing Issue

The events of September 11, 2001 have led to an almost universal acknowledgement in the United States Government of the need for consolidating and streamlining collection, analysis, and dissemination of information concerning threats to the United States and its interests. According to the President's National Strategy for Homeland Security ("the Strategy"), intelligence contributes to every aspect of homeland security and is a vital foundation for the homeland security effort. The Strategy recognizes that U.S. information technology is the most advanced in the world, but that our information systems have not adequately supported the homeland security mission. According to the Strategy, the U.S. government spends about $50 billion per year on information technology, but the systems purchased are not compatible between the agencies of the federal government, or with state and local entities. The Strategy also acknowledges that legal and cultural barriers often prevent agencies from exchanging and integrating intelligence and other information.

In response to these problems, the Strategy first calls for integrating information sharing across the federal government through the Critical Infrastructure Assurance Office (CIAO). Under this plan, the CIAO would design and implement an interagency information architecture to support efforts to find, track, and respond to terrorist threats. The CIAO would coordinate groups focusing on border and transportation security and other countermeasures to the use of weapons of mass destruction. As part of this effort, the FBI will create a consolidated Terrorism Watch List that includes information from both intelligence and law enforcement sources.

The Strategy also calls for integrating information sharing across state and local governments, private industry, and among the U.S. citizenry. Using modern information technology, more information is to be shared among various databases. The FBI and other agencies will augment information that currently is available in the National Crime Information Center databases and National Law Enforcement Telecommunications Systems. This information integration effort will require that Intelligence Community agencies make efforts to remove classified information from some documents in order to allow them to be shared with state and local officials.

Finally, the Strategy calls for the adoption of standards for information that is in electronic form and is relevant to homeland security. According to the Strategy, terrorist-related information from the databases of all government agencies with responsibilities for homeland security is to be integrated. The Department of Justice, FBI, and other federal agencies, and numerous state and local law enforcement agencies, will then be able to use data-mining tools to apply this information to the homeland security mission.

Major provisions of two of the homeland security-related bills now pending before Congress would promote the sharing of critical homeland security information regarding threats between federal intelligence agencies and law enforcement agencies as well as state and local officials, sheriffs, governors, mayors, other elected officials, and other emergency responders. The bills recognize the continuing need to protect sensitive sources and collection methods by granting security clearances to appropriate state and local personnel.

The bills would also direct the President to develop procedures by which federal agencies will share homeland security information with, and receive such information from state and local personnel. Further, the bills would require information sharing systems to have the capability to transmit classified or unclassified information, have the capability to restrict delivery of information based on the recipient's need to know, and be accessible to appropriate state and local personnel.

In recent years, a number of Commissions established by the Congress have reported on the ability of the United States to respond to terrorist events and have recommended that steps be taken to encourage closer cooperation between the intelligence and law enforcement communities. The hearings of this Joint Inquiry have shown that, although there is no information to indicate with certainty that the terrorist attacks of September 11, 2001 could have been prevented, some have suggested that certain terrorist acts may have been facilitated by continuing poor information exchanges between intelligence and law enforcement agencies and by blurred lines of organizational responsibility.

One of the mechanisms established by Congress, the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, looked very closely at the issues relating to the sharing of counter terrorism intelligence with state and local officials. The Advisory Panel was established by the National Defense Authorization Act for Fiscal Year 1999, and was chaired by then-Governor James Gilmore of Virginia who will be appearing as a witness today. The Advisory Panel issued three reports in December 1999, 2000, and 2001.

In its first report, the Advisory Panel reported that state and local officials had expressed a need for more intelligence, and for better information sharing among entities at all levels regarding potential terrorist threats. The report stated that, while the Panel was acutely aware of the need to protect classified national security information and the sources and methods by which it may have been obtained, it believed more could be done to provide timely information up, down, and laterally, at all levels of government to those who need the information to provide effective deterrence, interdiction, protection, and response to potential threats.

The Panel's second annual report stated that the potential connection between terrorism originating outside the United States and terrorist acts perpetrated inside the United States means that "foreign" terrorism may not be easily distinguished from "domestic" terrorism. The report urged that an even more comprehensive dissemination system than the JTTFs must be developed to provide information through expanded law enforcement channels for further dissemination to local response entities. In its third and final report, the Panel described the results of a survey it had commissioned that substantiated the panel's view that state and local entities are in need of threat assessments and better intelligence concerning potential terrorist activities.

The premise of the Panel throughout its work has been that all terrorist incidents are local, or at least will begin that way. The Panel recommended that a federal office for combating terrorism establish a system for providing clearances to state and local officials and that the FBI implement an analytic concept similar to the CIA's "Reports Officers" to do a better job of tracking and analyzing terrorism indicators and warnings.

GAO's Assessment Of Information Sharing Within And Between Federal, State, And Local Agencies

The General Accounting Office has completed a number of reports for Congress that focus on combating terrorism, information sharing, and homeland security. In addition, GAO's written statement for the record for this hearing emphasizes the need for a commitment by the leadership of the FBI, CIA, and other agencies to transform the law enforcement and intelligence communities and achieve the most effective information sharing possible to combat terrorism.

GAO has confirmed that, the FBI, CIA, NSA, and other agencies have distinct organizational cultures. Also, legal walls, classification walls, and historically-ingrained walls of bureaucratic practice exist between these agencies. As GAO views the situation, only with the commitment, effectiveness and persistence of strong and visionary managers, will these walls be brought down and greater amounts of information sharing occur.

The three problems of information sharing identified by GAO as important to resolve if national, state, and local governments are to succeed in their collective war on terrorism include fragmentation, technological impediments, and ineffective collaboration. The GAO's assessment regarding the importance of technological impediments is supported by the FBI's inability to share information among its field offices and headquarters and with other agencies. The problem of information fragmentation is also illustrated by the fact that the intelligence office at the Federal Aviation Administration now at the Transportation Security Administration (TSA)--received information indicating that reputed terrorist bomber Ahmed Ressam had been arrested while trying to enter the United States from Canada with the intent of bombing the Los Angeles International Airport. It then issued an analysis of the bomb equipment seized, but this analysis was not directly shared with the Intelligence Community at the same time that it was released to the airports and the airlines.

Additional Databases

The Joint Inquiry Staff has reviewed numerous databases that contain important financial, travel, and vital statistics information. The Staff also has been informed of other powerful search mechanisms that have not been tapped because agencies are not fully aware of their existence or capabilities.

For example, both INS at the Justice Department and the Diplomatic Security Service (DSS) at the State Department claim that their databases and capabilities were never fully exploited in the FBI's efforts to locate the two hijackers, al Mihdhar and al Hazmi, who were identified by CIA in August 2001 as having entered the United States. Individuals at both INS and DSS claim that they may have been able to locate the two hijackers before September 11, 2001, had they been provided with the full context of the search and all the intelligence that was available on the two hijackers.

The multiple databases that exist with the Intelligence Community cannot be discussed here because of national security classification. However, we can briefly describe some of the many unclassified databases and task forces that exist and are intended to facilitate sharing information among law enforcement agencies.

Selected Law Enforcement Databases

NCIC: The FBI's National Crime Information Center is a national index of theft reports, warrants, and other criminal justice information submitted by law enforcement agencies across the country. NCIC provides real-time notification of information regarding persons and property to police officers and law enforcement officials.

NLETS: NLETS is a nationwide network that links all states and many federal agencies together for the exchange of criminal justice information. In each state, an agency is responsible for maintaining in-state law enforcement telecommunication systems that deliver messages throughout the state. Each state's criminal justice system can access any other state's criminal justice system to obtain a variety of information, including vehicle registration, drivers license, and criminal history records. Other data includes plane, boat, and gun registrations.

TIPS: Terrorism Information and Prevention System, established by the FBI consists of a website and a toll free 800 number for reports of any information about possible terrorist crimes. The phone tip line received over 180,000 calls in less than two months and generated about 30,000 leads.

CODIS: Established by the FBI in 1990, the Combined DNA Index System is a national index of DNA profiles. It is a key tool for solving violent crimes by enabling federal, state, and local crime labs to exchange and compare DNA profiles electronically, thereby linking crimes to each other and to convicted offenders.

NIBIN: The National Integrated Ballistics Information Network attempts to unify Bureau of Alcohol, Tobacco, and Firearms and FBI firearms databases.

NDPIX: The National Drug Pointer Index is a system that allows state, local, and federal agencies to determine if a suspect is under investigation by any other participating agency.

TECS: Treasury's Enforcement Communications Systems is a computerized information system designed to identify individuals and businesses suspected of involvement in violations of federal law. TECS is also a communications system permitting message transmittal between Treasury law enforcement offices and other national, state, and local law enforcement agencies. TECS provides access to the FBI's National Crime Information Center (NCIC) and the National Law Enforcement

Telecommunication Systems (NLETS. with the capability of communicating directly with state and local enforcement agencies.

IBIS: The Interagency Border Inspection System assists border enforcement agencies in focusing their limited resources on potential non-compliant travelers at ports of entry. IBIS provides the law enforcement community with access to computer-based enforcement files of common interest. It also provides access to the FBI's National Crime Information Center (NCIC) and allows its users to interface with all fifty states via the National Law Enforcement Telecommunications Systems (NLETS). IBIS resides on the Treasury Enforcement Communications System (TECS) at the Customs Data Center. IBIS also contains the INS' NAILS database. An IBIS network with more than 24,000 computer terminals provides field-level access. These terminals are located at air, land, and sea ports of entry. IBIS keeps track of information on suspect individuals, businesses, vehicles, aircraft, and vessels. IBIS terminals can also be used to access NCIC records on wanted persons, stolen vehicles, vessels or firearms, license information, criminal histories, and previous Federal inspections. The information is used to assist law enforcement and regulatory personnel.

NAILS: The National Automated Immigration Lookout System is a central mainframe computer system that provides a reliable method of verifying the admissibility of an individual and preventing inadmissible individuals from entering the United States. NAILS facilitates inspection and investigation processes by providing quick and easy retrieval of biographical or case data on individuals who should not be permitted to enter the United States. Individual INS applications supply the data contained in NAILS II. Other information is provided by Federal, state, local, and foreign government agencies, and other entities.

SELECTED FEDERAL TASK FORCES

JTTF: Prior to September 11, 2001 there were thirty-four JTTFs nationwide that included members from federal agencies such as the U.S. Marshals Service, the U.S.

Department of State's Diplomatic Security Service, the Bureau of Alcohol Tobacco and Firearms, the Immigration and Naturalization Service, the U.S. Secret Service and local entities such as the New York State Police. After September 11, the Department of Justice established 56 JTTFs, one in each FBI field office, to enhance the FBI's ability to promote coordinated terrorism investigations among FBI field offices and law enforcement organizations nationwide. The JTTFs now involve over 3,700 agents, compared to 2,178 before September 11.

ATTF: To integrate and further coordinate antiterrorism activities in the field, the Justice Department created 93 Anti-Terrorism Task Forces, one in each U.S. Attorney's district—to integrate the communications and activities of local, state and federal law enforcement. The ATTFs include a 24 hour, seven day per week, contact system to ensure that key members of the ATTFs and other agencies can quickly communicate and respond to any future terrorist attacks.

FTTTF: The Foreign Terrorist Tracking Task Force was established to better ensure that federal agencies, including the FBI, INS, and Customs Service coordinate their efforts to bar from the United States and locate aliens who are suspected of engaging in terrorist activity, or who provide material support to terrorist activity.

Conclusion

In summary, the Joint Inquiry Staff believes that much information of great potential utility to the counterterrorism effort exists in the files and databases of many federal, state, and local agencies, as well as in the private sector. However, that information is not always shared or made available in timely and effective ways to those who are in a position to act upon it, add it to their analysis, and use it to better accomplish their individual missions. Our review found problems in maximizing the flow of relevant information both within the Intelligence Community as well as to and from those outside the Community. The reasons for these information disconnects can be, depending on the case, cultural, organizational, human, or technological. Comprehensive solutions, while perhaps difficult and costly, must be developed and implemented if we are to maximize our potential for success in the war against terrorism.