

Testimony of  
**Mr. Dennis Lormel**

October 9, 2002

Introduction

Good morning, Madam Chairman, and members of the Subcommittee on Technology, Terrorism, and Government Information. On behalf of the Federal Bureau of Investigation (FBI), I would like to express my gratitude to the Subcommittee for affording us the opportunity to participate in this forum and to update the Subcommittee on our use of the tools established within the framework of the USA PATRIOT Act and the work being conducted by our Terrorism Financing Operations Section.

As this Subcommittee is well aware, the FBI, in conjunction with law enforcement and intelligence agencies throughout the United States and the world, is engaged in the largest, most complex and perhaps the most critical criminal and terrorism investigation in our history. The FBI continues to dedicate considerable resources to this investigation and remains committed to determining the full scope of these terrorist acts, identifying all those involved in planning, executing and/or assisting in any manner the commission of these acts and others, and bringing those responsible to justice. The FBI will continue to exercise its leadership role in the global war on terrorism by taking all possible steps to prevent any further acts of terrorism.

The war on terrorism will be a long-term battle. It will not be won overnight nor will it be won without the highest levels of cooperation and coordination among law enforcement and intelligence agencies around the globe. Terrorism knows no borders or boundaries. The threat is not limited to any one region of the world. Law enforcement and intelligence agencies throughout the world possess tremendous resources and expertise. Allying these resources against the common enemy of terrorism is the key to dismantling these organizations and eliminating the threat they pose. Make no mistake about it, even with the combined resources and expertise possessed by law enforcement, the threat posed by terrorism is grave. Terrorists do not play by the rules of a civilized society, nor do they respect human decency. They will stop at nothing to commit acts of terror.

From a law enforcement perspective, success in the war on terrorism must be measured in our ability to prevent future acts of terrorism. Whether it be through prosecution, disruption, blocking/freezing of funds, or allowing a funding mechanism to remain in place in order to further an investigation, prevention remains the overarching focus. In this regard, fighting the war on terrorism requires powerful tools. The FBI appreciates the tools provided by the Congress in enacting the USA Patriot Act, including those contained within Title III of this Act, which is also known as the International Money Laundering Anti-Terrorist Financing Act of 2001.

## The Terrorist Financing Operations Section (TFOS)

I would like to start my discussion regarding the FBI's use of the USA Patriot by focusing on the tools provided within Title III. To illustrate how these anti-money laundering provisions aid our investigative efforts, it is necessary to understand how the FBI has been re-structured to address terrorist financing matters. Identifying and tracking the financial structure supporting terrorist groups is critical to dismantling the organization and preventing future attacks. As in ordinary criminal investigations, "following the money" identifies, links, and develops evidence against those involved in criminal activity. In the early stages of the investigation into the events of September 11, 2001, it was financial evidence that quickly established links between the hijackers and identified co-conspirators.

It was also in the early stages of this investigation that the FBI and Department of Justice (DOJ) identified a critical need for a more comprehensive, centralized approach to terrorist financial matters. In response, the FBI established an interagency Terrorism Financial Review Group (TFRG), operating out of FBI Headquarters. By bringing together vast databases and the expertise of numerous federal agencies, the TFRG, which was subsequently expanded, renamed the Terrorist Financing Operations Section (TFOS), and assigned to the FBI's Counterterrorism Division, focuses a powerful array of resources on the financial tentacles of terrorist organizations.

The TFRG was created with a two-fold mission. First, it was designed to conduct a comprehensive financial analysis of the 19 hijackers to link them together and to identify their financial support structure within the United States and abroad. Through the execution of this mission, the TFRG was able to establish how the hijackers responsible for the attacks received their money, details of their flight training, where they lived, and details concerning individuals associated with the hijackers. The 19 hijackers opened 24 domestic bank accounts at four different banks. The TFOS analyzed the data associated with these accounts to develop a financial profile that has been used in connection with the FBI's investigation regarding the events of September 11, 2001.

The second aspect of the TFRG's mission was to serve as a template for preventive and predictive terrorist financial investigations. This mission, consistent with the TFRG's restructuring into the TFOS, has since evolved into a broader effort to identify, investigate, prosecute, disrupt, and dismantle all terrorist-related financial and fund-raising activities.

To accomplish this mission, the TFOS has implemented initiatives to address all aspects of terrorist financing. For example, the TFOS is engaged in an aggressive international outreach program to share information regarding terrorist financing methods with the financial community and law enforcement, and has built upon long-established relationships with the financial services community in the United States and abroad. The international outreach initiative is coordinated through the network of FBI Legal Attache Offices located in 44 key cities worldwide, providing coverage for more than 200 countries and territories.

As touched upon earlier, a significant focus of the TFOS' efforts is prediction and prevention. In this regard, it has developed numerous data mining projects to provide further predictive abilities and maximize the use of both public and private database information. These efforts are complemented by the centralized terrorist financial database which the TFOS developed in

connection with its coordination of financial investigation of individuals and groups who are suspects of FBI terrorism investigations. The TFOS has cataloged and reviewed financial documents obtained as a result of numerous financial subpoenas pertaining to individuals and accounts. These documents have been verified as being of investigatory interest and have been entered into the terrorist financial database for linkage analysis. The TFOS has obtained financial information from FBI Field Divisions and Legal Attache Offices, and has reviewed and documented financial transactions. These records include foreign bank accounts and foreign wire transfers. The information contained within the aforementioned database is being used to identify terrorist cells operating in the United States and abroad to prevent further terrorist acts. The TFOS meets regularly with representatives from the banking community and the financial services industry to share information and to refine methods to detect and identify potential terrorists around the world.

The TFOS created and continues to update a financial control list which contains names and identifying data for individuals under investigation for potential links to terrorist organizations. These lists are regularly shared with domestic and international law enforcement and intelligence agencies, and with the Federal Reserve Board, which disseminates the lists to financial institutions so they can flag suspicious financial activity.

The TFOS regularly shares information with Customs' Operation Green Quest and provides daily downloads from its database to Green Quest and the Financial Crimes Enforcement Network (FinCEN). Further, the TFOS is working with FinCEN to explore new ways to data mine the Suspicious Activity Report (SAR), Currency Transaction Report (CTR), and Currency and Monetary Instrument Report databases.

Based on its international investigative abilities, and its close association with the Intelligence Community, the TFOS is in a unique position to coordinate anti-terrorism financial investigations and to ensure those investigations are coordinated with the goals and objectives of the FBI's Counterterrorism Program.

#### Use of the USA PATRIOT Act

I would now like to discuss how the TFOS has been making use of the tools established by the USA PATRIOT Act. Terrorist financing methods range from the highly sophisticated to the most basic. Traditionally, their efforts have been aided considerably by the use of correspondent bank accounts, private banking accounts, offshore shell banks, bulk cash smuggling, identity theft, credit card fraud, and other criminal operations. Informal Value Transfer Systems, such as "Hawalas," also present problems for law enforcement. They permit terrorists a means of transferring funds that is difficult to detect and trace. These informal systems are commonplace and appear to serve as an efficient means of transacting in mostly "cash" societies such as Pakistan, Afghanistan, and the Phillipines. In applying provisions of the USA PATRIOT Act we seek to erode the effectiveness of such methods without unduly undermining the legitimate economic activity that may rely on them. The Act establishes stricter rules for correspondent bank accounts, requires securities brokers and dealers to file SARs, and certain cash businesses to register with FinCEN and file SARs for a wider range of financial transactions.

The Act contains many other provisions that the FBI believes will considerably aid our efforts to address terrorist financing. These include the authority to seize terrorist assets, and the addition

of terrorism and other offenses to the list of racketeering offenses. The utilization of this aspect of the USA PATRIOT Act is perhaps best exemplified through actions that have been taken against Non-Governmental Organizations (NGOs) believed to provide financial support to known Foreign Terrorist Organizations and other affiliated Terrorist Cells. As in the case of Halawas, the funding of terrorist organizations such as Al Qaeda and Hamas through NGOs and charitable organizations represents a significant challenge to law enforcement. Funding of terrorism through NGOs is a prime focus of terrorist financial investigations. NGOs may be large international organizations which can be exploited by individual employees sympathetic to terrorist causes through local branch offices; they may be private NGOs which exist solely to support a militant cause; or they may be closely affiliated with a state sponsor of terrorism. One of the challenges in investigations involving terrorist fund-raising through NGOs is distinguishing terrorist fund-raising activities from legitimate or what may appear to be legitimate charitable fund-raising. Fund-raising on the part of terrorist groups which on the surface appear to be efforts to "help the poor" or fund-raising for charitable, humanitarian or other legitimate purposes actually falls squarely in the realm of logistical support for terrorist activity.

As a participant on the National Security Council's Policy Coordinating Committee (PCC) on terrorist finance, the TFOS participates in the effort to target NGOs believed to provide financial support to known Foreign Terrorist Organizations and affiliated terrorist cells. The PCC coordinates the development and implementation of policies to combat terrorist financing and provides analysis on these issues. Numerous FBI Field Offices have open investigations into organizations that may be funneling money to Foreign Terrorist Organizations and the TFOS has acted as a clearinghouse for these cases and has summarized the collected data.

In order to disrupt terrorist financing channels, the TFOS has coordinated FBI terrorist investigations with the terrorist designation and asset freezing efforts of the OFAC and Operation Green Quest. These efforts have resulted in the freezing of millions of dollars in foreign and US bank accounts. Specifically, the joint efforts targeting Al-Barakaat, the Holy Land Foundation for Relief and Development, the Global Relief Foundation, and the Benevolence International Foundation have resulted in the execution of numerous search warrants and the disruption of the fund-raising and money remittance operations of these and other organizations. Financial investigations of these entities have revealed that approximately \$200 million in contributions passed through these organizations each year.

The USA PATRIOT Act also enables prosecutors to seize money subject to forfeiture in a foreign bank account by authorizing the seizure of a foreign bank's funds held in a U.S. correspondent account. Other important provisions expand the ability to prosecute unlicensed money transmitters, allow law enforcement faster access to reports of currency transactions in excess of \$10,000, and provide authority for the service of administrative subpoenas on foreign banks concerning records of foreign transactions. This latter provision allows law enforcement to obtain critical information in an investigation on a more timely basis than was possible before. In counterterrorism investigations, of course, speed is of the essence because prevention is the goal. Section 362 of the USA PATRIOT Act mandates that FinCEN establish a highly secure network to 1) allow financial institutions to file SARs and CTRs on-line, and 2) "provide financial institutions with alerts and other information regarding suspicious activities that warrant

immediate and enhanced scrutiny." FinCEN has developed the USA Patriot Act Communication System to meet this mandate and is implementing the system. This will be a valuable tool for law enforcement, but it will require the full cooperation of private financial institutions. The TFOS has worked with financial institutions, and has provided to them information to help detect patterns of activity possibly associated with terrorist activity and the PACS will help considerably in these efforts.

#### Use of Other Provisions of the USA PATRIOT Act

In addition to the provisions effecting changes to money laundering statutes, the USA PATRIOT Act effected changes in national security authorities, the substantive criminal law, immigration law, and victim assistance statutes, and other areas. In particular, the Act seeks to improve the efficiency of the process associated with the FBI's conduct of electronic surveillance and physical searches authorized through the Foreign Intelligence Surveillance Act (FISA) of 1978 and to remove barriers to the timely sharing of information between counterintelligence and counterterrorism intelligence operations and criminal investigations. These enhancements in efficiency improve our ability to detect and prosecute offenders, and with less disruption to legitimate commerce. I would now like to highlight those provisions that the FBI has been utilizing most often in connection with the execution of its counterterrorism responsibilities.

#### Changes in Predicate Standards for National Security Letters (NSLs)

NSLs are administrative subpoenas that are issued in counterintelligence and counterterrorism investigations to obtain telephone and electronic communications records from telephone companies and Internet Service Providers (pursuant to the Electronic Communications Privacy Act, or ECPA); records from financial institutions (pursuant to the Right to Financial Privacy Act); and information from credit bureaus (pursuant to the Fair Credit Reporting Act). Delay in obtaining NSLs has long been identified as a significant problem relative to the conduct of counterintelligence and counterterrorism investigations. Two factors contributed most prominently to this delay. These were the complexity of the standard predication for NSLs and the requirement that signature authority be restricted to officials no lower than a Deputy Assistant Director at FBI Headquarters.

Section 505 of the USA Patriot changed the standard predication for all three types of NSLs to one requiring that the information being sought through the NSL is "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment of the Constitution of the United States." Prior to the Act, the statutes required both relevance and "specific and articulable facts" giving reason to believe that the subject is an agent of a foreign power, or, in the case of subscriber requests, had been in contact with such an agent. This "agent of a foreign power" prong of the standard made it necessary to collect and document specific facts demonstrating that the standard had been met. This requirement and the complexity of the standard itself often led to extensive delays in generating NSLs.

Section 505 also allowed the Director to delegate signature authority for NSLs to Special Agents in Charge serving in designated field divisions. The provisions delineated within Section 505

have resulted in investigators receiving the data needed in the furtherance of ongoing investigations in a more timely fashion, which in turn has had a positive impact on numerous investigations.

#### "Roving" FISA Electronic Surveillance Authority

Section 206 of the USA PATRIOT Act amends FISA to allow the FISC to issue a "generic" secondary order where the Court finds that the "actions of the target of the application may have the effect of thwarting the identification of a specified person." This means that, when a FISA target engages in conduct that has the effect of defeating electronic surveillance, such as by rapidly switching cell phones, Internet accounts, or meeting venues, the Court can issue an order directing "other persons," to effect the authorized electronic surveillance.

#### Changes in the Duration of FISA Authority

Section 207 of the Act extends the standard duration for several categories of FISC Orders. First, the section allow for electronic surveillances and search orders on non-US person agents of a foreign power pled under Section 101(b)(1)(A) of the FISA, to run for an initial period of 120 days, instead of 90, and to be renewed for periods of one year. The section also extends the standard duration of physical search orders in all other cases, which applies to US persons and non-officer/employee targets, from 45 to 90 days. These extension provisions have resulted in a more effective utilization of available personnel resources and the collection mechanisms authorized under the FISA.

#### Expansion of the FISC

Section 207 also expanded the FISC from seven judges to eleven judges, three of whom must reside in the Washington, D.C. area. This has increased the availability of FISC judges and has resulted in the convening of the FISC on a weekly basis, which has enabled the FBI to implement FISA-authorized collection operations in a more timely fashion.

#### Changes in FISA Pen Register/Trap and Trace Authority

Section 214 of the Act makes a substantial revision to the standard for a FISA-authorized pen register/trap and trace. Prior to the USA PATRIOT Act, FISA-authorized pen registers required two showings: (1) relevance to an investigation, and (2) specific and articulable facts giving reason to believe that the targeted line was being used by an agent of a foreign power, or was in communications with such an agent, under specified circumstances. Section 214 simply eliminates the second of the required showings. FISA-authorized pen/trap and trace orders are now available whenever the FBI certifies that "the information likely to be obtained is foreign intelligence information not concerning a United States person, or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution."

This new standard requires that the information sought be relevant to an "ongoing investigation to protect against international terrorism or clandestine intelligence activities." Use of this technique is authorized in full investigations properly opened under the AG Guidelines for FBI

Foreign Intelligence Collection and Foreign Counterintelligence Investigations. Finally, the new standard does not mean that FISA pen register/trap and trace authority is only available on the subjects of investigations. The authority is available when the information sought is "relevant" to the investigation, as described above. For example, information concerning apparent associates or, or individuals in contact with, the subject of an investigation, may be relevant.

## Conclusion

The USA PATRIOT Act has provided the FBI with improved tools for conducting counterterrorism and counterintelligence investigations. These new tools require DOJ and the FBI to gain a complete understanding of the provisions, develop guidelines and protocols for their appropriate use, and educate investigators and prosecutors. In addition, many of the provisions require the Department of Treasury to issue new regulations and rules. While all of this is being done as expeditiously as possible, the full impact of the tools provided by the USA PATRIOT Act are yet to be seen. The FBI is continuing to digest its provisions, develop guidelines and protocols for its appropriate use, and educate investigators and prosecutors. Nevertheless, the Act enhances the ability of law enforcement and intelligence agencies to achieve our common goal of preventing acts of terrorism, without compromising the civil liberties and Constitutional protections enjoyed by our citizens. Thank you for this opportunity to appear today. I welcome any questions you have.