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 unlicenced 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.

b2 [redacted]

"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.

[Congressional Matters Index] [OPA Home]

Testimony of Robert S. Mueller, III

Director, Federal Bureau of Investigation

Before the United States Senate

Committee on the Judiciary

May 20, 2004

Good morning Mr. Chairman, Senator Leahy, and Members of the Committee. I am pleased to be here today to update you on the FBI's substantial progress in the counterterrorism and intelligence arenas since my last appearance before the Committee. I would also like to acknowledge that the progress the FBI has made in reforming our counterterrorism and intelligence programs is due in no small part to the enactment of the USA PATRIOT Act.

Every day, the men and women of the FBI demonstrate their determination to fulfill the great responsibility that you, and the public, have entrusted to them. As a result, the FBI has made steady progress in meeting our highest priority of preventing terrorism. The terrorist threat presents complex challenges. Terrorists move easily across international borders, use sophisticated technology to recruit, network, and communicate, and finance their operations with elaborate funding schemes. Above all, they are patient. They are methodical. They are determined to succeed.

But the FBI is equally determined to succeed. To defeat these threats, the FBI must have several critical capabilities: First, we must develop intelligence about terrorist activity and use that intelligence to disrupt their plans. Second, we must be global – we must work closely with our counterparts at home and abroad to develop and pool our collective knowledge and expertise. Third, we must use cutting-edge information technology to collect, analyze, manage, and share our information effectively. Most importantly, we must work within the framework of the Constitution, protecting our cherished civil liberties as we work to protect the American people.

Today, I would like to give you a brief overview of the steps we have taken to put these critical capabilities in place by reforming our counterterrorism and intelligence programs, as well as overhauling our information technology. Before I begin, however, I would like to acknowledge that none of our successes would have been possible without the extraordinary efforts of our partners in state and municipal law enforcement and our counterparts around the world. The Muslim, Iraqi, and Arab-American communities have also contributed a great deal to the war on terror. On behalf of the FBI, I would like to thank these communities for their assistance and for their ongoing commitment to preventing acts of terrorism. The country owes them a debt of gratitude.

PATRIOT ACT

Mr. Chairman, for over two and a half years, the PATRIOT Act has proved extraordinarily beneficial in the war on terrorism and has changed the way the FBI does business. Many of our counterterrorism successes, in fact, are the direct results of provisions included in the Act, a number of which are scheduled to "sunset" at the end of next year. I strongly believe it is vital to our national security to keep each of these provisions intact. Without them, the FBI could be forced back into pre-September 11 practices, attempting to fight the war on terrorism with one hand tied behind our backs.

Let me give you just a few examples that illustrate the importance of the PATRIOT Act to our counterterrorism efforts:

First and foremost, the PATRIOT Act – along with the revision of the Attorney General's investigative guidelines and the 2002 decision of the Foreign Intelligence Surveillance Court of Review – tore down the wall that stood between the intelligence investigators responding to terrorist threats and the criminal investigators responding to those same threats.

- Prior to September 11, an Agent investigating the intelligence side of a terrorism case was barred from discussing the case with an Agent across the hall who was working the criminal side of that same investigation. For instance, if a court-ordered criminal wiretap turned up intelligence information, the criminal investigator could not share that information with the intelligence investigator – he could not even suggest that the intelligence investigator should seek a wiretap to collect the information for himself. If the criminal investigator served a grand jury subpoena to a suspect's bank, he could not divulge any information found in those bank records to the intelligence investigator. Instead, the intelligence investigator would have to issue a National Security Letter in order to procure that same information.

- The removal of the "wall" has allowed government investigators to share information freely. Now, criminal investigative information that contains foreign intelligence or counterintelligence, including grand jury and wiretap information, can be shared with intelligence officials. This increased ability to share information has disrupted terrorist operations in their early stages -- such as the successful dismantling of the "Portland Seven" terror cell – and has led to numerous arrests, prosecutions, and convictions in terrorism cases.

- In essence, prior to September 11th, criminal and intelligence investigators were attempting to put together a complex jigsaw puzzle at separate tables. The Patriot Act has fundamentally changed the way we do business. Today, those investigators sit at the same table and work together on one team. They share leads. They fuse information. Instead of conducting parallel investigations, they are fully integrated into one joint investigation.

- Because of the creation of the Terrorist Threat Integration Center, and because the FBI has dramatically improved its information sharing with the CIA, the NSA, and a host of other federal, state, local and international partners, our resources are used more effectively, our investigations are conducted more efficiently, and America is immeasurably safer as a result. We cannot afford to go back to the days when Agents and prosecutors were afraid to share information.

Second, the PATRIOT Act gave federal judges the authority to issue search warrants that are valid outside the issuing judge's district in terrorism investigations. In the past, a court could only issue a search warrant for premises within the same judicial district – yet our investigations of terrorist networks often span multiple districts. The PATRIOT Act streamlined this process, making it possible for judges in districts where activities related to terrorism may have occurred to issue search warrants applicable outside their immediate districts.

In addition, the PATRIOT Act permits similar search warrants for electronic evidence such as email. In the past, for example, if an Agent in one district needed to obtain a search warrant for a subject's email account, but the Internet service provider (ISP) was located in another district, he or she would have to contact an AUSA and Agent in the second district, brief them on the details of the investigation, and ask them to appear before a judge to obtain a search warrant – simply because the ISP was physically

NSL VIO-2910

-b2

based in another district. Thanks to the PATRIOT Act, this frustrating and time-consuming process can be averted without reducing judicial oversight. Today, a judge anywhere in the U.S. can issue a search warrant for a subject's email, no matter where the ISP is based.

Third, the PATRIOT Act updated the law to match current technology, so that we no longer have to fight a 21st-century battle with antiquated weapons. Terrorists exploit modern technology such as the Internet and cell phones to conduct and conceal their activities. The PATRIOT Act leveled the playing field, allowing investigators to adapt to modern techniques. For example, the PATRIOT Act clarified our ability to use court-ordered pen registers and trap-and-trace devices to track Internet communications. The Act also enabled us to seek court-approved roving wiretaps, which allow investigators to conduct electronic surveillance on a particular suspect, not a particular telephone – this allows them to continuously monitor subjects without having to return to the court repeatedly for additional authorizations. This technique has long been used to investigate crimes such as drug trafficking and racketeering. In a world in which it is standard operating procedure for terrorists to rapidly change locations and switch cell phones to evade surveillance, terrorism investigators must have access to the same tools.

In a final example, the PATRIOT Act expanded our ability to pursue those who provide material support or resources to terrorist organizations. Terrorist networks rely on individuals for fund-raising, procurement of weapons and explosives, training, logistics, and recruiting. The material support statutes allow investigators to aggressively pursue and dismantle the entire terrorist network, from the financiers to those who carry out terrorist plans. By criminalizing the actions of those who provide, channel, or direct resources to terrorists, the material support statutes provide an effective tool to intervene at the earliest possible stage of terrorist planning. This allows the FBI to arrest terrorists and their supporters before their deadly plans can be carried out.

For instance, the FBI investigated a case in Charlotte, North Carolina, in which a group of Lebanese nationals purchased mass quantities of cigarettes in North Carolina and shipped them to Michigan for resale. Their scheme was highly profitable due to the cigarette tax disparity between the two states. The proceeds of their smuggling were used to fund Hezbollah affiliates and operatives in Lebanon. Similarly, the FBI investigated a case in San Diego in which subjects allegedly negotiated with undercover law enforcement officials the sale of heroin and hashish in exchange for Stinger anti-aircraft missiles, which they indicated were to be sold to Al Qaida. In both cases, the material support provisions allowed prosecutors to charge the subjects and secure guilty pleas and convictions.

Mr. Chairman and Members of the Committee, the importance of the PATRIOT Act as a valuable tool in the war against terrorism cannot be overstated. It is critical to our present and future success. By responsibly using the statutes provided by Congress, the FBI has made substantial progress in its ability to proactively investigate and prevent terrorism and protect innocent lives, while at the same time protecting civil liberties.

COUNTERTERRORISM AND INTELLIGENCE PROGRAM REFORMS

Let me turn for a few moments to the progress the FBI has made in strengthening and reforming its counterterrorism and intelligence programs to support its number one goal of terrorism prevention. Today, the FBI is taking full advantage of our dual role as both a law enforcement and an intelligence agency. Let me give you just a few examples of the progress we have made:

• We have more than doubled the number of counterterrorism Agents, intelligence analysts, and linguists.

• We expanded the Terrorism Financing Operations Section, which is dedicated to identifying, tracking, and cutting off terrorist funds.

• We are active participants in the Terrorist Threat Integration Center and the Terrorist Screening Center, which provides a new line of defense against terrorism by making information about known or suspected terrorists available to federal, state, and local law enforcement.

• We have worked hard to break down the walls that have sometimes hampered our coordination with our partners in federal, state and local law enforcement. Today, the FBI and CIA are integrated at virtually every level of our operations. This cooperation will be further enhanced when our Counterterrorism Division co-locates with the CIA's Counter Terrorist Center and the multi-agency Terrorist Threat Integration Center.

• We expanded the number of Joint Terrorism Task Forces (JTTF) from 34 to 84 nationwide.

• We created and refined new information sharing systems, such as the National Alert System, that electronically link us with our domestic partners.

• We have sent approximately 275 FBI executives to the Kellogg School of Management at Northwestern University to receive training on executive leadership and strategic change.

Recognizing that a strong, enterprise-wide intelligence program is critical to our success across all investigations, we have worked relentlessly to develop a strong intelligence capability and to integrate intelligence into every investigation and operation across the FBI:

• We stood up the Office of Intelligence, under the direction of a new Executive Assistant Director for Intelligence. The Office of Intelligence sets unified standards, policies, and training for analysts, who examine intelligence and ensure it is shared with our law enforcement and intelligence partners. The Office of Intelligence has already provided over 2,600 intelligence reports and other documents for the President and members of the Intelligence Community.

• We established a formal analyst training program. We are accelerating the hiring and training of analytical personnel, and developing career paths for analysts that are commensurate with their importance to the mission of the FBI.

• We developed and are in the process of executing Concepts of Operations governing all aspects of the intelligence process – from the identification of intelligence requirements to the methodology for intelligence assessment to the drafting and formatting of intelligence products.

• We established a Requirements and Collection Management Unit to identify intelligence gaps and develop collection strategies to fill those gaps.

• We established Reports Officers positions and Field Intelligence Groups in the field offices, whose members review investigative information – not only for use in investigations in that field office – but to disseminate it throughout the FBI and among our law enforcement and Intelligence Community partners.

With these changes in place, the Intelligence Program is established and growing. We are now turning to the last structural step in our effort to build an intelligence capacity. In March, I authorized new procedures governing the recruitment, training, career paths and evaluation of our Special Agents – all of which are focused on developing intelligence expertise among our agent population.

The most far-reaching of these changes will be the new agent career path, which will guarantee that agents get experience in intelligence investigations and with intelligence processes. Under this plan, new agents will spend an initial period familiarizing themselves with all aspects of the Bureau, including intelligence collection and analysis, and then go on to specialize in counterterrorism, intelligence or another operational program. A central part of this initiative will be an Intelligence Officer Certification program that will be available to both analysts and agents. That program will be modeled after – and have the same training and experience requirements as – the existing programs in the Intelligence Community.

INFORMATION TECHNOLOGY IMPROVEMENTS

All the progress the FBI has made on all investigative fronts rests upon a strong foundation of information technology. Over the past two and a half years, the FBI has made tremendous efforts to overhaul our information technology, and we have made significant progress.

• Over 1,000 counterterrorism and counterintelligence FBI Headquarters employees have been provided with access to Top Secret/Sensitive Compartmented Information (TS/SCI) information at their desks.
• We implemented the Wide Area Network and the Enterprise Operations Center on schedule in March 2003.

• We improved data warehousing technology to dramatically reduce stove-piping and cut down on man-hours that used to be devoted to manual searches.

• The Full Site Capability deployment began in February of this year, and was completed on April 29th. Altogether, nearly 30,000 workstations have been converted to the new Trilogy baseline software and new email system.

• We now have a permanent Chief Information Officer and Chief Technology Officer, who oversee the development and management of all IT projects and systems throughout the FBI. It is important to keep in mind that Trilogy is not the FBI's sole IT system – the FBI has over 200 IT systems, all of which must be maintained, enhanced when necessary, and certified and accredited for security.

As you know, during the past year we have encountered some setbacks regarding the deployment of Trilogy's Full Site Capability (FSC) and the Virtual Case File. Our goal is to deliver Virtual Case File capabilities by the end of this year. You are aware that last week, the National Research Council of the National Academies (NRC) released a report reviewing the Trilogy IT Modernization program. The FBI commissioned this review as part of our ongoing efforts to improve our capabilities to assemble, analyze and disseminate investigative and operational data both internally and externally with other intelligence and law enforcement agencies.

Many of the NRC's recommendations have already been implemented or are a work in progress. The FBI has repeatedly sought outside evaluation and advice throughout its IT modernization efforts and will continue to do so. The NRC report specifically noted that the counterterrorism mission requires extensive information sharing, and recommended

NSL VIO-2913

that the FBI involve other agencies in its modernization program. We will continue to work closely with other Department of Justice Agencies and members of the Homeland Security and Intelligence Communities to ensure the FBI has the right technology to support information sharing and other mission requirements.

CONCLUSION

With our counterterrorism, intelligence, and information technology initiatives firmly in place, the FBI is moving steadily forward, always looking for ways to evolve and improve so that we remain a step ahead of our enemies. We are looking at ways to assess and adjust our resource needs based on threats, in order to ensure that we have the personnel and resources to meet and defeat all threats.

Mr. Chairman, I would like to commend the men and women of the FBI for their hard work and dedication – dedication both to defeating terrorism and to upholding the Constitution. They have embraced and implemented the counterterrorism and intelligence reforms I have outlined for you today and they are committed to upholding their duty to protect the citizens of the United States.

Mr. Chairman, thank you again for the Committee's support of the FBI and for the opportunity to be here this morning.

I would be happy to answer any questions you might have.

[Congressional Matters Index] [OPA Home]

As I have described above, the USA Patriot Act has been invaluable in providing the FBI with tools that it needs to fight terrorism in the 21st Century. This committee has been one of our strongest supporters in this effort and for this the men and women of the FBI are grateful. Having said that, I would like to address another area in which the FBI needs the committee's support in order to continue to fulfill its primary mission of protecting America from further terrorist attacks.

Administrative Subpoenas

Planning, funding, supporting and committing acts of terrorism all are federal crimes. For many years, the FBI has had administrative subpoena authority for investigations of crimes ranging from drug trafficking to health care fraud to child exploitation. Yet, when it comes to terrorism investigations, the FBI has no such authority.

Instead, we rely on two tools – National Security Letters (NSLs) and orders for FISA business records. Although both are useful and important tools in our national security investigations, administrative subpoena power would greatly enhance our abilities to obtain information. Information that may be obtained through an NSL is limited in scope and enforcement is difficult. FISA business record requests require the submission of an application for an order to the FISA Court. In investigations where there is a need to obtain information expeditiously, Section 215, which does not contain an emergency provision, may not be the most effective process to undertake. The administrative subpoena power would be a valuable complement to these tools and provide added efficiency to the FBI's ability to investigate and disrupt terrorism operations and our intelligence gathering efforts. It would provide the government with an enforcement mechanism which currently does not exist with NSLs. Moreover, it would bring the authorities of agents and analysts investigating terrorism into line with the authorities the FBI already has to combat other serious crimes. I would like to stress that the administrative subpoena power proposal should provide the recipient the ability to quash the subpoena on the same grounds as a grand jury subpoena.

CONCLUSION

Mr. Chairman and Members of the Committee, the importance of the provisions of the USA Patriot Act I have discussed today in the war against terrorism cannot be overstated. They are crucial to our present and future successes. By responsibly using the statutes provided by Congress, the FBI has made substantial progress in its ability to proactively investigate and prevent terrorism and protect lives, while at the same time protecting civil liberties. In renewing those provisions scheduled to "sunset" at then end of this year, Congress will ensure that the FBI will continue to have the tools it needs to combat the very real threat to America posed by terrorists and their supporters. In addition, by giving the FBI administrative subpoena authority, Congress will enable the FBI to be more efficient in its Counterterrorism efforts. Thank you for your time today. I am happy to answer any of your questions.

Statement
of
ROBERT S. MUELLER, III
Director
Federal Bureau of Investigation

Before The
United States Senate
Committee on the Judiciary

July 27, 2005

Good morning, Mr. Chairman, Senator Leahy, and Members of the Committee. I am pleased to appear before you today to update you on recent changes within the FBI and to address additional changes we anticipate in the near future. I would like to thank the Committee for your oversight of the FBI and your interest in ensuring our success in carrying out our mission.

I would like to take this opportunity before the Committee to discuss the President's recent announcement of the creation of an intelligence service within the FBI. This service will unify the FBI's Directorate of Intelligence, Counterterrorism Division, and Counterintelligence Division and will integrate FBI intelligence and investigative operations more fully into the broader Intelligence Community. Within this context, I would like to address three areas that directly impact the success of this new intelligence service: our Language Program, our Information Technology capabilities, and our ability to recruit, hire, train, and retain the expertise we need to build this service. Finally, Mr. Chairman, I would like to take this opportunity to reiterate the FBI's need for administrative subpoena authority in support of our efforts in the war on terrorism.

FBI Organization

Last month, the President announced that he had approved certain recommendations of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (the WMD Commission). While the WMD Commission recognized that the FBI has made substantial progress in building our intelligence program, it expressed concern that our existing structure did not give the Director of National Intelligence (DNI) the ability to ensure that our intelligence functions are fully integrated into the Intelligence Community.

We are currently preparing a plan for implementing the President's directive to establish an intelligence service within the FBI. While the details of this plan are currently being discussed with the Department of Justice and the Office of the DNI, I would like to share with the Committee the broad concepts under which this service is being developed.

One guiding principle of the FBI's intelligence program, as implemented by the Directorate of Intelligence, has been the integration of the FBI's intelligence and investigative missions. An FBI intelligence service will build on the progress of the Directorate of Intelligence and further promote this integration. The integration of our intelligence and investigative missions ensures that intelligence drives investigative operations. Further, this integration enables the FBI to capitalize on its established investigative capacity to collect information and to extend that strength to the analysis and production of intelligence. This intelligence service will integrate intelligence and investigative operations by combining our counterterrorism, counterintelligence and foreign intelligence investigative components with our intelligence component and by placing the service under the supervision of a single official who will report to the Deputy Director.

The development of a specialized national security workforce is a key component of this new service. We will develop this workforce through initiatives, many of which are already in place, designed to recruit, hire, train and retain investigative and intelligence professionals who have the skills necessary to the success of our national security programs. For example, in accordance with the Intelligence Reform Act, our Directorate of Intelligence has established a specialized and integrated national intelligence workforce, which consists of intelligence analysts, language analysts, and physical surveillance specialists, as well as 500 Special Agents. To support this workforce, we are developing an intelligence career service that addresses the full range of human resource issues from hiring to training to professional development and retention.

Finally, the creation of an intelligence service within the FBI will enhance our ability to coordinate our national security activities with the DNI and the rest of the Intelligence Community. The single FBI official in charge of the intelligence service will be able to ensure that we direct our national security resources in coordination with the DNI, who will have the authority to concur in the appointment of this official.

Mr. Chairman, this is a broad outline of our plans for an intelligence service within the FBI. I am happy to provide the Committee additional details as the implementation of this initiative progresses.

Directorate of Intelligence: Foreign Language Program (FLP)

Prior to September 11, 2001, translation capabilities, like most other FBI programs, were decentralized and managed in the field. Post 9/11, we established the Language Services Translation Center (LSTC) at FBI Headquarters to provide centralized management of the Foreign Language Program. The LSTC provides a command and control structure at FBI Headquarters to ensure that our translator resource base of over 1,300 translators, distributed across 52 field offices, is strategically aligned with priorities set by our operational divisions and with national intelligence priorities.

We have now integrated Language Services into the Directorate of Intelligence. This integration fully aligns the FBI's foreign language and intelligence management activities and delivers a cross-cutting platform for future improvements across all program areas, including translation quality controls. We are also in the process of integrating linguists into our Field Intelligence Groups (FIGs) in each field office where their roles are expected to expand to include more intelligence reporting and analysis. Integration into the FIGs will establish a clear chain of command for the management and development of our language personnel. And, as their roles change, FBI linguists will receive greater training opportunities and Language Analysts will have greater promotion potential within the organization.

In addition, we have instituted prioritization processes to ensure that foreign language collection is translated in accordance with a clear list of priorities. The Foreign Language Program receives regular weekly updates to FISA prioritization. We are careful to ensure that the FBI's priorities are consistent with those set by the FISA prioritization board established by the Director of Central Intelligence. Our participation in this board has served to ensure our compliance in this area.

We also use a triage system to sift through collected materials. Once a document is received, a linguist quickly provides a cursory review and sets aside documents with pertinent information for future translation/summary. On audio lines that are mixed with several languages, a linguist reviews all the calls and forwards the foreign language sessions to the appropriate linguist for review and summary of pertinent sessions. We also route specific intelligence collection through the DI's English Monitoring Center (EMC) There, English Monitor/Analysts (EM) review the collection, summarize and report pertinent English materials, and forward the remaining foreign language items to the appropriate linguists across the country. This process allows our linguists to concentrate on the review, analysis, translation, and reporting of foreign language materials. On some audio FISA materials, where we are looking for a particular piece of information, a linguist will do a quick review and triage the audio for future translation.

With regard to the translation backlog, Mr. Chairman, we currently possess sufficient translation capability to promptly address all of our highest priority counterterrorism intelligence, generally within 24 hours. This prioritization and triage process has helped us reduce our accrued backlog. Of the several hundred thousand hours of audio materials and several million pages of text collected in connection with counterterrorism investigations over the last two years, only 1.8% of all audio (8,354 hours out of a total of 418,855 hours collected), 0.8% of all electronic data files (36,667 files out of 4,104,134 files collected), and less than 0.1%

text (149 pages out of a total of 1,833,347 pages collected) exist as accrued backlog.

Since the Office of the Inspector General completed its audit, we have reviewed more than 95% of all counterterrorism audio collected (403,864 hours out of a total of 426,593 collected). We found that 93% of the accrued backlog is attributable to either elongated "white noise" microphone recordings from certain techniques not expected to yield intelligence of tactically high value (4,668 hours of open microphone recording out of the total audio backlog of 8,354, or 56% of the backlog) or to audio from highly obscure languages and dialects that we are currently recruiting and hiring to address (3,362 hours due to a obscure languages out of the total audio backlog of 8,354, or 40% of the backlog).

We currently have translation capabilities in approximately 100 languages. The languages in the backlog are so rare that, in some cases, we have found that there is no one within the Intelligence Community with a proficiency in the language. We have addressed this issue through intense recruiting efforts, and have hired 9 additional linguists in one very rare language.

Mr. Chairman, I would also like to address some of the Inspector General's concerns about linguist hiring, vetting, and training. Since 9/11, we have recruited and processed more than 50,000 translator applicants. These efforts have resulted in the addition of 877 new Contract Linguists (net gain of 554 after attrition) and 112 new Language Analysts (net gain of 27 after attrition). The FBI has increased its overall number of linguists by 69%, with the number of linguists in certain high priority languages, such as Arabic, increasing by more than 200 percent.

At the same time, however, we must ensure translation security and quality. All FBI translator candidates are subject to a pre-employment vetting process that eliminates over 90% of those who apply.

There are currently over 3,000 FBI employees and contractors who have certified foreign language proficiency scores at or above Level II - basic working proficiency - including 406 Language Analysts and 959 Contract Linguists.

More than 95% of the FBI's linguists are native speakers of their foreign language and hold Top Secret security clearances. Their native-level fluencies and long-term immersions within a foreign culture ensure not only a firm grasp of colloquial and idiomatic speech, but also of heavily nuanced language containing religious, cultural, and historical references. Beyond these qualities, over 80% of FBI linguists hold at least a bachelor's degree and 37% hold a graduate-level degree. These qualities make them extremely valuable to the FBI's intelligence program, but also particularly attractive to other employers seeking these scarce skill sets. Strong demand for their language skills from other government agencies and the private sector is well documented. It is due in large part to this demand and competition that annual attrition among FBI Language Analysts has risen to approximately 7% since 9/11. Our attrition rate for contract linguists is approximately 11%.

We are also working to increase the language proficiency of other FBI employees. We have made added investments to our language training and cultural awareness programs. Last year alone, our Foreign Language Training Program provided training and/or self-study materials to 1,470 FBI employees in 32 languages.

The FBI meets the need for Special Agent linguists by hiring agents who already have language skills, and also by offering agents training in critical foreign languages. Special Agents are proficient in 45 foreign languages, and there are currently 1,340 Special Agents who have Level 2 foreign language proficiency, including 35 Agents who speak Arabic. The Language Training Program component of the DI's Training and Oversight Unit provides high-quality, cost effective foreign language and language-related training to Special Agents whose jobs require them to use foreign languages, work with non-Roman alphabets, or have an understanding of foreign cultures.

The FBI Directorate of Intelligence manages the Special Agent Linguist Program and the language training that supports agent linguist requirements. The Special Agent Linguist Program assesses the deployment of Special Agents who are proficient in a foreign language and recommends permanent and temporary placement of new and experienced agents with foreign language proficiency in response to the FBI's investigative and intelligence priorities. Special Agents proficient in foreign languages are assigned to field offices, legal attaches, FBI Headquarters and the FBI Academy.

We have also taken steps to ensure proper security and continuing quality from the linguists we bring onboard. We have instituted a post-adjudication risk management program that mandates periodic personnel security interviews, polygraph examinations, and database access audits for each FBI translator. In the event this process discloses questionable or inappropriate associations based on self-reporting, or if such associations are brought to our attention by a third party, a security assessment is immediately conducted by the appropriate field office squad in coordination with our Security Division. Whenever credible and serious allegations surface, the translator's access to FBI space and information is suspended.

While we share the OIG's concerns regarding our quality control procedures, we are strengthening them by instituting national Translation Quality Control (QC) Policy and Guidelines. The FBI's QC Program requires that, after an initial week of intense training, all work performed by new linguists during their first 40 hours of service is subject to review by a senior linguist. Work performed during the second 80 hours of service will also be heavily spot-checked, and later checked with decreasing frequency as required. In all, it is estimated that each new linguist hired or contracted by the FBI will require an investment of at least 120 hours by a senior linguist dedicated to QC.

Mr. Chairman, we recognize that the FBI's foreign language program is key to the success of both the FBI's intelligence and law enforcement missions. We appreciate the oversight by this Committee and by the OIG and look forward to working with you in ensuring that we have the translation capabilities we need to address the many threats we face as a nation.

FBI Information Technology

Mr. Chairman, we recognize that the ability to assemble, analyze, and disseminate information both internally and with other intelligence and law enforcement agencies is essential to our success in the war on terrorism. As a result, we have made modernization of our Information Technology (IT) a priority and have developed a coordinated, strategic approach to IT under the centralized leadership of the Office of the Chief Information Officer (OCIO).

The OCIO has developed a Strategic IT Plan, a baseline Enterprise Architecture, and a system for managing IT projects at each stage of their "life cycle" from planning and investment, through development and deployment, operation and maintenance, and disposal. In addition, the OCIO has been working closely with the OIG to address its recommendations for achieving our IT goals. We have made substantial progress in each of these areas:

- The need for a sound program management structure
- The need for establishment and enforcement of appropriate processes
- The need for Life Cycle Management controls and process
- The need for an empowered Chief Information Officer
- The need for Portfolio Management and Investment Management
- The need for an Enterprise Architecture
- The need for a Strategic Information Technology Plan

The modernization of our IT capabilities will be completed in the form of a Service-Oriented-Architecture (SOA). "Sentinel" will be one such service, or, more accurately, a suite of services geared to evolve with our new and emerging needs, to work within and take advantage of the infrastructure, equipment and networking improvements effected by the Trilogy Program. The Trilogy Program was planned as a modernization effort for system infrastructure, network optimization, and upgrade or replacement of the five most important FBI investigative applications supporting the field. At the same time, as these efforts got underway, current events radically changed the mission focus and, consequently, the information to support the new focus. This resulted in new and emerging requirements, including the need for better collaboration, complex workflow analysis and tracking programs, and a critical need for information sharing.

Sentinel is not the Virtual Case File (VCF) which, as we know, suffered from inadequate management control, new and changing requirements, and the inability to maintain pace with these technical requirements. Sentinel differs from VCF in that it will serve as the platform from which services can be gradually deployed, each deployment offering added improvements. Sentinel will pave the road, starting with our legacy case management system, for subsequent transformation of all legacy applications to modern technology under our Enterprise Architecture. Services to be provided by Sentinel are currently planned for deployment in four phases, each phase providing standalone capabilities, each incrementally developed and deployed. In this manner, as each phase is developed, lessons learned from earlier deployments can be leveraged to our advantage. Early next year, initial development will begin; the full deployment of all services supporting our information management needs is anticipated to take a little over 40 months.

Mr. Chairman, I am aware that the Committee is interested in the estimated total cost of the Sentinel program. At this time, cost estimates are considered "source selection information" as defined by the Federal Acquisition Regulation, meaning that any public disclosure might improperly affect the bidding process. The FBI is committed to obtaining the best product at the lowest cost to the American people and we do not want to prematurely disclose information which may influence bids from potential contractors.

Human Resources

The men and women of the FBI are our most valuable asset. In order to continue to recruit, hire, train, and retain quality individuals for our expanding human capital needs, we have undertaken a re-engineering of our human resource program.

- We have retained the services of an outside consulting firm to review of business processes for selection and hiring, training and development, performance management, Intelligence Officer certification, retention, and career progression.

- We have removed non-human resource functions, such as facilities management, from the Administrative Services Division to create a pure human resource function.

- We have hired an executive search firm to identify a Chief Human Resources Officer for the FBI with significant experience in transformation of HR processes in a large organization.

- We have made substantial progress in building a specialized and integrated Intelligence Career Service comprised of Intelligence Analysts, Language Analysts, Physical Surveillance Specialists, and Special Agents.

- We have developed a Special Agent career path that will be implemented in October 2005. These career paths will take into account the background and experience of the Agent in determining the Agent's future career path in one of five programs: Counterterrorism, Counterintelligence, Intelligence, Cyber, or Criminal. This policy will promote the FBI's interest in developing a cadre of Special Agents with subject matter expertise.

These are just a few of the initiatives underway to improve the FBI's human capital and to ensure that we develop a workforce that is prepared to meet the challenges of the future.

Administrative Subpoenas

Mr. Chairman, when I last appeared before the Committee, my prepared testimony included a request for administrative subpoena authority in support of our counterterrorism efforts. I was remiss in not including that request in my oral remarks and would like to take the opportunity to do so at this time.

As you know, the FBI has had administrative subpoena authority for investigations of crimes ranging from drug trafficking to health care fraud to child exploitation. Yet, when it comes to terrorism investigations, the FBI has no such authority.

Instead, we rely on National Security Letters (NSLs) and FISA orders for business records. Although both are useful and important tools in our national security investigations, administrative subpoena power would greatly enhance our abilities to obtain information. Information that may be obtained through an NSL is limited in scope and enforcement is difficult because the request is in the form of a letter, not a subpoena or court order. FISA business record requests, although delivered in the form of a court order, require the submission of an application for an order to the FISA Court. This is a time-consuming process and, in investigations where there is a need to obtain information expeditiously, a FISA order for business records, which does not contain an emergency provision, may not be the most effective process to undertake.

As a result, we submit that the administrative subpoena would be a valuable complement to these tools and provide added efficiency to the FBI's ability to investigate and disrupt terrorism operations and our intelligence gathering efforts. It would provide the government with an enforcement mechanism which currently does not exist with NSLs and it would provide the expediency not available with a FISA business records order. Moreover, it would bring the authorities of agents and analysts investigating terrorism into line with the authorities the FBI already has to combat other serious crimes. I would like to stress that the administrative subpoena power proposal would provide the recipient the ability to quash the subpoena on the same grounds as a grand jury subpoena.

Conclusion

Mr. Chairman and Members of the Committee, thank you again for this opportunity to discuss these important issues concerning the transformation of the FBI. Much has been accomplished. Much remains to be done. But our strategic plan, our methodology and process improvements are guiding our prioritization and performance in support of the FBI mission.

I am happy to answer any questions you may have.

National Security Law Policy and Training Unit

Unit Chief [redacted]
Room 7947 JEH
202-324-[redacted]

b6
b7C
b2

---

1 November 2005

Re: <u>NSL Talking Points for General Counsel</u>

National Security letters are administrative requests that allows the FBI to obtain certain limited types of information without the requirement of prior court intervention:

1) Under the **Electronic Communications Privacy Act, 18 U.S.C. § 2709**, the FBI can obtain telephone and email communication records from telephone companies and internet service providers.

2) Under the **Right to Financial Privacy Act, 12 U.S.C. § 3414(a)(5)(A)**, the FBI can obtain the records of financial institutions (which is very broadly defined).

3) Under the **Fair Credit Reporting Act, 15 U.S.C. §§ 1681u(a) and (b)**, the FBI can obtain a list of financial institutions and consumer identifying information from a credit reporting company.

4) Under the **Fair Credit Reporting Act, 15 U.S.C. § 1681v**, the FBI can obtain a full credit report in a counterterrorism case. This provision was created by the 2001 USA Patriot Act.

The standard for issuing an NSL is **relevance** 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. (The 1681v NSL standard is slightly different to reflect that it applies only to international terrorism investigations.)

Statute	Type of NSL	Reporting Requirement
Electronic Communications Privacy Act 18 U.S.C. §2709(e)	•Telephone Subscriber or Electronic Subscriber information (limited to name, address, and length of service). •Telephone local and long distance toll billing records. •Electronic Communication Transactional Records (e.g. transaction/activity logs and e-mail header information).	Semiannual Reporting
Right to Financial Privacy Act 12 U.S.C. § 3414(a)(5)	•Financial Records	Semiannual Reporting
Fair Credit Reporting Act 15 U.S.C. § 1681u(a) & (b)	•Consumer identifying Information. • Identity of Financial Institution.	Semiannual Reporting
Fair Credit Report Act 15 U.S.C. § 1681v	•Full credit reports from credit bureau.	No reporting requirement under the Fair Credit Reporting Act.

2. NY NSL Litigation - ACLU Lawsuit Regarding NSLs:

b6
b7C
b2

Talking Points attached (POC [redacted]

Large portions of the NY district court case are still under seal, but the district court's decision and order are not and can be discussed. Some information in the appellate briefs is also under seal. The type of information that cannot be discussed publicly includes the name of and specific details (e.g., location) regarding the NSL recipient, as well as the facts underlying the investigation giving rise to the NSL. We have also been keeping the identity and FO of the agent who served the NSL confidential.

3. Connecticut Litigation regarding NSL:

b6
b7C
b2

POCs [redacted] [redacted]

- John Doe, ACLU, American Civil Liberties Union Foundation v. Alberto Gonzales, in his official capacity as AG of the US; Robert Mueller, in his official capacity as Director of the FBI, and John Roe, FBI, in his official capacity. CIVIL ACTION NO. 3.05-cv-1256 (JCH) D. Conn [Doe v. Gonzales]

•Challenge to service of an ECPA NSL on a library consortium.

•District of Proceeding: District Court, Connecticut (Hartford)

•Stage of Proceeding:

•On September 9, 2005, District Court issued preliminary injunction against defendants enforcing non-disclosure provision; Defendants appealed.

•On September 20, 2005, Second Circuit (No. 05-4896) issued stay of that order pending appeal.

•On September 22, 2005, plaintiffs filed emergency motion to vacate Second Circuit's stay pending appeal.

•On September 29, 2005, Second Circuit denied plaintiffs' emergency motion to vacate stay.

•On October 7, 2005, Supreme Court (Circuit Justice Ginsburg) denied plaintiffs' motion to vacate stay .

•On November 2, 2005, merits of expedited appeal by defendants from preliminary injunction to be argued before Second Circuit (along with the Southern District of New York case where the court found the ECPA NSL statute unconstitutional).

•On November 10, 2005, government answer to complaint due in district court (expect government will move for further stay of proceedings pending disposition of Second Circuit appeal).

National Security Law Policy and Training Unit

Unit Chief [redacted]
Room 7947 JEH
202-32[redacted]

b6
b7C
b2

Talking Points re Washington Post article of November 6, 2005.

I. NSL Information:

A. Statutory Authority:

National Security letters are administrative requests that allow the FBI to obtain certain limited types of information without the requirement of prior court intervention:

1) Under the **Electronic Communications Privacy Act, 18 U.S.C. § 2709**, the FBI can obtain telephone and email communication records from telephone companies and internet service providers.

2) Under the **Right to Financial Privacy Act, 12 U.S.C. § 3414(a)(5)(A)**, the FBI can obtain the records of financial institutions (which is very broadly defined).

3) Under the **Fair Credit Reporting Act, 15 U.S.C. §§ 1681u(a) and (b)**, the FBI can obtain a list of financial institutions and consumer identifying information from a credit reporting company.

4) Under the **Fair Credit Reporting Act, 15 U.S.C. § 1681v**, the FBI can obtain a full credit report in a counterterrorism case. This provision was created by the 2001 USA Patriot Act.

Statute	Type of NSL	Reporting Requirement
Electronic Communications Privacy Act 18 U.S.C. §2709(e)	•Telephone Subscriber or Electronic Subscriber information (limited to name, address, and length of service). •Telephone local and long distance toll billing records. •Electronic Communication Transactional Records (e.g. transaction/activity logs and e-mail header information).	Semiannual Reporting
Right to Financial Privacy Act 12 U.S.C. § 3414(a)(5)	•Financial Records	Semiannual Reporting
Fair Credit Reporting Act 15 U.S.C. § 1681u(a) & (b)	•Consumer identifying Information. • Identity of Financial Institution.	Semiannual Reporting
Fair Credit Report Act 15 U.S.C. § 1681v	•Full credit reports from credit bureau.	No reporting requirement under the Fair Credit Reporting Act.

B. <u>FBI's Use of NSLs Post-USA PATRIOT Act</u>:

•The standard for issuing an NSL is **relevance** 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. (The 1681v NSL standard is slightly different to reflect that it applies only to international terrorism investigations.)

•The new "relevance" standard resulted in the increase in the number of NSLs issued by the FBI to further its investigations.

•NSLs are used as preliminary building block of an investigation - like grand jury subpoenas and FISA section 215 business records orders.

•NSLs are limited to the described categories of records. If the information sought falls outside of these categories, the FBI must use another investigative tool (e.g., grand jury subpoena or 215 order).

C. <u>Process</u>:

•A request for an NSL has two parts. One is the NSL itself, and one is the EC approving issuance of the NSL.

•The cover EC serves four functions. It documents the predication for the NSL by stating why the information sought is relevant to an authorized investigation. It documents the approval of the NSL by field supervisors. It contains information needed to fulfill Congressional reporting requirements for each type of NSL (subject's USP status, type of NSL issued, and the number of phone numbers, email addresses, account numbers or individual records being requested in the NSL). Lastly, it transmits the NSL to NSLB for reporting requirements, to CTD, CD, or Cyber for informational purposes, and, in the case of personal service, to the requesting squad or delivering field division for delivery.

II. Comparison of National Security Letters pre and post-USA PATRIOT Act:

A. Standard:

Pre-USA PATRIOT Act	Post-USA PATRIOT Act
Specific and articulable facts standard •The pre-USA PATRIOT Act standard for the issuance of an NSL required the records be **relevant to an authorized foreign counterintelligence investigation** and that the FBI have **specific and articulable facts** that the requested records **related to an agent of a foreign power or a foreign power**. •Put differently, the FBI had to have reached a defensible position that the person was a terrorist or spy before the FBI could gather the base information it needed to determine whether the person was a terrorist or spay. •The standard was unreasonably high. An NSL is clearly analogous to a grand jury subpoena, which can be issued during a criminal investigation to obtain relevant information. It would be anomalous if it were easier to obtain these sorts of record in a routine criminal investigation than in an investigation to protect the national security.	**Relevance** Standard (Section 505) The standard for issuing an NSL is **relevance** to an authorized investigation– •to protect against international terrorism; or, •clandestine intelligence activities; and •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.

B. Approval Authority for NSLs:

Pre-USA PATRIOT Act	Post-USA PATRIOT Act
Approval authority could be no lower than Deputy Assistant Director	The authority to sign NSLs has been delegated to: • the Deputy Director and Executive Assistant Director for CT/CI; •Assistant Directors in charge and all DADs for CT/CI/Cyber (except that CI and Cyber ADs and DADs do not have any authority with respect to 1681v NSLs); •General Counsel; •Deputy General Counsel for National Security Affairs; •Assistant Directors in Charge in NY, D.C., and LA; and, •all SACs (An acting SAC may not sign an NSL).

C. Retention/Dissemination of NSL Information:

Pre-USA PATRIOT Act	Post-USA PATRIOT Act
•As stated, FBI Policy pre and post USA PATRIOT Act has been to maintain the information derived from NSLs regardless of whether it turns out to be relevant (for example - FBI determines that a target is not a threat). CTD mandates that all telephone information go into Telephone Applications.	•Information obtained through the use of an NSL may be retained and disseminated in accordance with general standards set forth in The Attorney General's Guidelines for FBI National Security Investigation and Foreign Intelligence Collection (NSIG). •FBI Policy pre and post USA PATRIOT Act has been to maintain the information derived from NSLs regardless of whether it turns out to be relevant (for example - FBI determines that a target is not a threat). CTD mandates that all telephone information go into Telephone Applications.
•Dissemination is further subject to specific statutory limitations:	•Dissemination is further subject to specific statutory limitations:
•Privacy Act regarding U.S. Person information;	•Privacy Act regarding U.S. Person information;
• toll record NSL statute, ECPA, 18 U.S.C. §2709, and financial record NSL statute, RFPA, 12 U.S.C. §3414(a)(5)(B), permit dissemination if per NSIG and information is clearly relevant to responsibilities of recipient agency;	• toll record NSL statute, ECPA, 18 U.S.C. §2709, and financial record NSL statute, RFPA, 12 U.S.C. §3414(a)(5)(B), permit dissemination if per NSIG and information is clearly relevant to responsibilities of recipient agency;
•limited credit information NSL statute, FCRA, 15 U.S.C. §1681u, permits dissemination to other federal agencies as may be necessary for the approval or conduct of an FCI investigation; and,	•limited credit information NSL statute, FCRA, 15 U.S.C. §1681u, permits dissemination to other federal agencies as may be necessary for the approval or conduct of an FCI investigation; and,
•no special statutory rules for dissemination under full credit report NSL statute, FCRA, 15 U.S.C. §1681v.	•no special statutory rules for dissemination under full credit report NSL statute, FCRA, 15 U.S.C. §1681v.

III. Congressional Reporting? What? When?:

Statute	Reporting Requirement
Electronic Communications Privacy Act 18 U.S.C. §2709(e)	Semiannual Reporting: For toll billing/electronic communication transactional records the FBI reports – •Total NSLs re Non-US Persons. •Total # of investigations of different Non-USPs. •Total NSLs re US Persons. •Total # of investigations of different USPs. For subscriber information, the FBI only reports # of NSLs.
Right to Financial Privacy Act 12 U.S.C. § 3414(a)(5)	Semiannual Reporting: For requests for financial records, the FBI reports – •Total NSLs re Non-US Persons. •Total # of investigations of different Non-USPs. •Total NSLs re US Persons. •Total # of investigations of different USPs.
Fair Credit Reporting Act 15 U.S.C. § 1681u(a) & (b)	Semiannual Reporting For requests for financial institution and consumer identifying information, and consumer credit reports, the FBI reports– •NSLs re Non-US Persons. •NSLs re USPs.
Fair Credit Report Act 15 U.S.C. § 1681v	No reporting requirement under the Fair Credit Reporting Act.

The FBI does not have a reporting requirement for full credit reports under the Fair Credit Reporting Act (15 U.S.C. § 1681v). For the other NSLs, the FBI complies with semiannual reporting requirement as required by statute.

IV. Problems with NSLs:

•NSLs limited to specific categories of information (limited by statute).

•NSLs can be unreliable in time-sensitive investigations since the FBI often encounters delays in the process.

National Security Law Policy and Training Unit

Unit Chief [redacted]
Room 7947 JEH
202-324-[redacted]

b6
b7C
b2

[redacted]

b5

b5

b5

b5

National Security Law Policy and Training Unit

Unit Chief [redacted]
Room 7947 JEH
202-324[redacted]

b6
b7C
b2

---

8 November 2005

NATIONAL SECURITY LETTERS

I. **Defined**:

•National Security letters are a specific type of administrative request that allows the FBI to obtain **certain limited types of information** without court intervention:

1) Under the **Electronic Communications Privacy Act, 18 U.S.C. §2709**, the FBI can obtain telephone and email communication records from telephone companies and internet service providers.

2) Under the **Right to Financial Privacy Act, 12 U.S.C.§3414(a)(5)(A)**, the FBI can obtain the records of financial institutions (which is very broadly defined).

3) Under the **Fair Credit Reporting Act, 15 U.S.C.§§1681u(a) and (b)**, the FBI can obtain a list of financial institutions and consumer identifying information from a credit reporting company.

4) Under the **Fair Credit Reporting Act, 15 U.S.C. §1681v**, the FBI can obtain a full credit report in an international terrorism case. This provision was created by the 2001 USA Patriot Act.

•NSLs are used as preliminary building block of an investigation - like grand jury subpoenas and FISA section 215 business records orders.

•NSLs are limited to the described categories of records. If the information sought falls outside of these categories, the FBI must use another investigative tool (e.g., grand jury subpoena or 215 order).

Statute	NSL - Use and Type of Information Obtained	Date Available to FBI[1]
Electronic Communications Privacy Act 18 U.S.C. § 2709(e)	• Telephone subscriber or Electronic subscriber information (limited to name, address, and length of service). •Telephone local and long distance toll billing records. • Electronic communications transactional records (transaction/activity logs and e-mail header information).	1986
Right to Financial Privacy Act 12 U.S.C. § 3414(a)(5)	• Financial records.	1978
Fair Credit Reporting Act 15 U.S.C. § 1681u(a) 15 U.S.C. § 1681u(b)	• Consumer identifying information. • Identity of financial institution.	1996
Fair Credit Reporting Act 15 U.S.C. § 1681v	• Full credit reports from credit bureau.	2001

II. **Relevance Standard**:

The standard for issuing an NSL is relevance:

• 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

[1] Source: CRS Report for Congress dated April 15, 2005 - Administrative Subpoenas and National Security Letters in Criminal and Foreign Intelligence Investigations: Background and Proposed Adjustments.

of the Constitution of the United States. (The 1681v NSL standard is slightly different to reflect that it applies only to international terrorism investigations.)

Prior to the Patriot Act, the standard for issuance of an NSL was that the target or the communication was tied to a foreign power. That is no longer the case.

III. **Approval Authority**:

The authority to sign NSLs has been delegated to:

• the Deputy Director and Executive Assistant Director for CT/CI;

•Assistant Directors in charge and all DADs for CT/CI/Cyber (except that CI and Cyber ADs and DADs do not have any authority with respect to 1681v NSLs);

•General Counsel;

•Deputy General Counsel for National Security Affairs;

•Assistant Directors in Charge in NY, D.C., and LA; and,

•all SACs (An acting SAC may not sign an NSL).

IV. **Dissemination**:

•Information obtained through the use of an NSL may be disseminated in accordance with general standards set forth in The Attorney General's Guidelines for FBI National Security Investigation and Foreign Intelligence Collection (NSIG).

•Dissemination is further subject to specific statutory limitations:

• toll record NSL statute, ECPA, 18 U.S.C. §2709, and financial record NSL statute, RFPA, 12 U.S.C. §3414(a)(5)(B), permit dissemination if per NSIG and information is clearly relevant to responsibilities of recipient agency;

•limited credit information NSL statute, FCRA, 15 U.S.C. §1681u, permits dissemination to other federal agencies as may be necessary for the approval or conduct of an FCI investigation; and,

•no special statutory rules for dissemination under full credit report NSL statute, FCRA, 15 U.S.C. §1681v.

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

November 23, 2005

The Honorable Arlen Specter
Chairman
Committee on the Judiciary
United States Senate
Washington, D.C.

Dear Mr. Chairman:

On November 8, 2005, FBI General Counsel Valerie Caproni provided a classified briefing for Committee staff concerning the FBI's use of National Security Letters (NSLs). Enclosed are copies of the NSL templates used by the FBI. These documents, requested by staff members during the briefing, are provided in furtherance of your oversight activities. We request that you consult with this office prior to any further dissemination of this material.

We appreciate the opportunity to provide this additional information relating to this critically important tool. We welcome any feedback and look forward to continued cooperation in the interest of national security. Please contact me if we can assist you further on this or any other matter.

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 06-29-2007 BY 65179dmh/ksr/maj

Sincerely,

Eleni P. Kalisch
Assistant Director
Office of Congressional Affairs

The Honorable Patrick J. Leahy
Ranking Member
Committee on the Judiciary
United States Senate
Washington, D.C.

Enclosures

[DRAFTING DIVISION]
[STREET ADDRESS]
[CITY, STATE, ZIP CODE]
[MONTH, DAY, YEAR]

[MR./MRS./MS.] [COMPLETE NAME OF POC]
[TITLE, IF AVAILABLE]
[NAME OF COMPANY]
[PHYSICAL STREET ADDRESS - NO P.O. BOX]
[CITY, STATE - NO ZIP CODE]

DEAR [MR./MRS./MS.] [LAST NAME]:

Under the authority of Executive Order 12333, dated December 4, 1981, and pursuant to Title 15, United States Code (U.S.C.), Section 1681u(a) (the Fair Credit Reporting Act, as amended), you are hereby requested to provide the Federal Bureau of Investigation (FBI) the names and addresses of all financial institutions (as defined in Title 12, U.S.C., Section 3401) at which the below-named consumer(s) maintains or has maintained an account:

NAME(S):

ADDRESS(ES): [if available]

DATE(S) OF BIRTH: [if available]

SOCIAL SECURITY NUMBER(S): [if available]

In accordance with Title 15, U.S.C., Section 1681u(a), I certify that such information is sought for the conduct of an authorized investigation to protect against clandestine intelligence activities; and that such an investigation of a United States person is not conducted solely on the basis of activities protected by the First Amendment to the Constitution of the United States.

Please be advised that Title 15, U.S.C., Section 1681u(d), prohibits any consumer reporting agency, or officer from disclosing to any person that the FBI has sought or obtained access to information or records under these provisions. In addition, no consumer reporting agency, or officer, employee or agent of such consumer reporting agency, may include in any consumer report any information that would indicate that the FBI has sought or obtained such information.

You are requested to provide records responsive to this request **[personally to a representative of the [DELIVERING DIVISION]** OR **through use of a delivery service to [OFFICE OF ORIGIN]]** within [xxxx] business days of receipt of this request.

Any questions you have regarding this request should be directed only to the **[[DELIVERING DIVISION]** OR **[OFFICE OF ORIGIN], depending on whether service is personal or through a delivery service]**. Due to security considerations, you should neither send the records through routine mail service nor disclose the substance of this request in any telephone conversation.

Your cooperation in this matter is greatly appreciated.

Sincerely yours,

[ADIC/SAC NAME]
[ASSISTANT DIRECTOR IN CHARGE/ SPECIAL AGENT IN CHARGE]

[DRAFTING DIVISION]
[STREET ADDRESS]
[CITY, STATE, ZIP CODE]
[MONTH, DAY, YEAR]

[MR./MRS./MS.] [COMPLETE NAME OF POC]
[TITLE, IF AVAILABLE]
[NAME OF COMPANY]
[PHYSICAL STREET ADDRESS - NO P.O. BOX]
[CITY, STATE - NO ZIP CODE]

DEAR [MR./MRS./MS.] [LAST NAME]:

Under the authority of Executive Order 12333, dated December 4, 1981, and pursuant to Title 15, United States Code (U.S.C.), Section 1681u(b) (the Fair Credit Reporting Act, as amended), you are hereby requested to provide the Federal Bureau of Investigation (FBI) the names, address, former addresses, places of employment, or former places of employment of the below-named consumer(s):

NAME(S):

ADDRESS(ES): **[if available]**

DATE(S) OF BIRTH: **[if available]**

SOCIAL SECURITY NUMBER(S): **[if available]**

In accordance with Title 15, U.S.C., Section 1681u(a), I certify that such information is sought for the conduct of an authorized investigation to protect against clandestine intelligence activities, and that such an investigation of a United States person is not conducted solely on the basis of activities protected by the First Amendment to the Constitution of the United States.

Please be advised that Title 15, U.S.C., Section 1681u(d), prohibits any consumer reporting agency, or officer from disclosing to any person that the FBI has sought or obtained access to information or records under these provisions. In addition, no consumer reporting agency, or officer, employee or agent of such consumer reporting agency, may include in any consumer report any information that would indicate that the FBI has sought or obtained such information.

You are requested to provide records responsive to this request **[personally to a representative of the [DELIVERING DIVISION]** OR **through use of a delivery service to [OFFICE OF ORIGIN]]** within [xxxx] business days of receipt of this request.

Any questions you have regarding this request should be directed only to the [**[DELIVERING DIVISION]** OR **[OFFICE OF ORIGIN]**,_**depending on whether service is personal or through a delivery service]**. Due to security considerations, you should neither send the records through routine mail service nor disclose the substance of this request in any telephone conversation.

Your cooperation in this matter is greatly appreciated.

Sincerely yours,

[ADIC/SAC NAME]
[ASSISTANT DIRECTOR IN CHARGE/
SPECIAL AGENT IN CHARGE]

[DRAFTING DIVISION]
[STREET ADDRESS]
[CITY, STATE, ZIP CODE]
[MONTH, DAY, YEAR]

[MR./MRS./MS.] [COMPLETE NAME OF POC]
[TITLE, IF AVAILABLE]
[NAME OF COMPANY]
[PHYSICAL STREET ADDRESS - NO P.O. BOX]
[CITY, STATE - NO ZIP CODE]

Dear **[MR./MRS./MS.] [LAST NAME]**:

Pursuant to Executive Order 12333, dated December 4, 1981, and 15 U.S.C. § 1681v of the Fair Credit Reporting Act, you are hereby directed to provide the Federal Bureau of Investigation (FBI) with a copy of a consumer credit report and all other information contained in your files for the below-listed consumer(s):

NAME(S):

ADDRESS(ES): **[if available]**

DATE(S) OF BIRTH: **[if available]**

SOCIAL SECURITY NUMBER(S): **[if available]**

In accordance with Title 15, U.S.C. § 1681v, I certify that I have been designated to make this request and that the requested information is necessary to conduct an authorized investigation of, or intelligence or counterintelligence activities or analysis related to, international terrorism.

Please be advised that 15 U.S.C. § 1681v(c) prohibits your consumer reporting agency or any officer, employee or agent of your agency from disclosing to any person that the FBI has sought or obtained access to information or records under these provisions. Furthermore, your agency, or any officer, employee or agent of your agency, is prohibited from including in any consumer report any information that would indicate or disclose that the FBI has sought or obtained such information.

You are requested to provide records responsive to this request **[personally to a representative of the [DELIVERING DIVISION]** OR **through use of a delivery service to [OFFICE OF ORIGIN]]** within [xxxx] business days of receipt of this request.

Any questions you have regarding this request should be directed only to the **[[DELIVERING DIVISION]** OR **[OFFICE OF ORIGIN]**, **depending on whether service is personal or through a delivery service]**. Due to security considerations, you should neither send the records through routine mail service nor disclose the substance of this request in any telephone conversation.

Your cooperation in this matter is appreciated.

Sincerely,

[ADIC/SAC NAME]
[ASSISTANT DIRECTOR IN CHARGE/ SPECIAL AGENT IN CHARGE]

[DRAFTING DIVISION]
[STREET ADDRESS]
[CITY, STATE, ZIP CODE]
[MONTH, DAY, YEAR]

[MR./MRS./MS.] [Complete name]
[TITLE, IF AVAILABLE]
[NAME OF COMPANY]
[PHYSICAL STREET ADDRESS - NO P.O. BOX]
[CITY, STATE - NO ZIP CODE]

Dear **[MR./MRS./MS.] [LAST NAME]**:

Under the authority of Executive Order 12333, dated December 4, 1981, and pursuant to Title 18, United States Code (U.S.C.), Section 2709 (Section 201 of the Electronic Communications Privacy Act of 1986) (as amended, October 26, 2001), you are hereby requested to provide to the Federal Bureau of Investigation (FBI) the name, address, and length of service for the below-listed **[e-mail/IP]** address holder(s):

[E-mail/IP ADDRESS or ADDRESSES]

[ON A SPECIFIC DATE]

or [FOR THE PERIOD FROM [SPECIFIC DATE] TO [SPECIFIC DATE]

or [PRESENT]]

If the time period noted above is to the "present," that term is intended to request information to the date of the processing of this request. If providing information to the date of processing is not feasible, please provide information to the date of receipt of this request.

In accordance with Title 18, U.S.C., Section 2709(b), I certify that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, and that such an investigation of a United States person is not conducted solely on the basis of activities protected by the First Amendment to the constitution of the United States.

You are further advised that Title 18, U.S.C., Section 2709(c), prohibits any officer, employee or agent of yours from disclosing to any person that the FBI has sought or obtained access to information or records under these provisions.

You are requested to provide records responsive to this request **[personally to a representative of the [DELIVERING DIVISION]** OR **through use of a delivery service to [OFFICE OF ORIGIN]]** within [xxxx] business days of receipt of this request.

Any questions you have regarding this request should be directed only to the **[[DELIVERING DIVISION]** OR **[OFFICE OF ORIGIN], depending on whether service is personal or through a delivery service]**. Due to security considerations, you should neither send the records through routine mail service nor disclose the substance of this request in any telephone conversation.

Your cooperation in this matter is greatly appreciated.

Sincerely yours,

[ADIC/SAC NAME]

[ASSISTANT DIRECTOR IN CHARGE/ SPECIAL AGENT IN CHARGE]

[DRAFTING DIVISION]
[STREET ADDRESS]
[CITY,STATE, ZIP CODE]
[MONTH DAY, YEAR]

[MR./MRS/MS.] [COMPLETE POC NAME]
[TITLE, IF AVAILABLE]
[COMPANY NAME]
[PHYSICAL STREET ADDRESS - NO P.O. BOX]
[CITY, STATE - NO ZIP CODE]

DEAR [MR./MRS./MS.] [LAST NAME]:

Under the authority of Executive Order 12333, dated December 4, 1981, and pursuant to Title 12, United States Code (U.S.C.), Section 3414(a)(5), (as amended, December 13, 2003), you are hereby directed to produce to the Federal Bureau of Investigation (FBI) all financial records pertaining to the customer(s) and/or accounts listed below:

NAME(S) [if available]

ACCOUNT NUMBER(s): [if available]

SOCIAL SECURITY NUMBER(S): [if available]

DATE(S) OF BIRTH: [if available]

[FOR PERIOD FROM INCEPTION TO PRESENT]

or [FOR PERIOD FROM [SPECIFIC DATE] TO [SPECIFIC DATE]

or [PRESENT]]

If the time period noted above is to the "present," that term is intended to request information to the date of the processing of this request. If providing information to the date of processing is not feasible, please provide information to the date of receipt of this request.

Please see the attachment following this request for the types of information that your financial institution might consider to be a financial record.

In accordance with Title 12, U.S.C. Section 3414(a)(5)(A), I certify that the requested records are sought for foreign counterintelligence investigation purposes to protect against international terrorism or clandestine intelligence activities, and that such an investigation of a United States person is not conducted solely on the basis of activities protected by the First Amendment to the Constitution of the United States.

In accordance with Title 12, U.S.C., Section 3403(b), I certify that the FBI has complied with all applicable provisions of the Right to Financial Privacy Act.

Please be advised that Title 12, U.S.C., Section 3414(a)(5)(D), prohibits any financial institution, or officer, employee or agent of such institution, from disclosing to any person that the FBI has sought or obtained access to a customer's or entity's financial records under this statute.

You are requested to provide records responsive to this request **[personally to a representative of the [DELIVERING DIVISION]**_OR **through use of a delivery service to the [OFFICE OF ORIGIN]]** within [xxxx] business days of receipt of this request.

Any questions you have regarding this request should be directed only to the **[[DELIVERING DIVISION]** OR **[OFFICE OF ORIGIN],_depending on whether service is personal or through a delivery service]**. Due to security considerations, you should neither send the records through routine mail service nor disclose the substance of this request in any telephone conversation.

Your cooperation in this matter is greatly appreciated.

Sincerely,

[ADIC/SAC NAME]
[ASSISTANT DIRECTOR IN CHARGE/
SPECIAL AGENT IN CHARGE]

ATTACHMENT

In preparing your response to this National Security Letter, you should determine whether your company maintains the following types of information which may be considered by you to be a financial record in accordance Title 12, United States Code, Section 3401(2):

[redacted]

b2
b7E

b2
b7E

[DRAFTING DIVISION]
[STREET ADDRESS]
[CITY, STATE, ZIP CODE]
[MONTH, DAY, YEAR]

[MR./MRS./MS.] [COMPLETE NAME OF POC]
[TITLE, IF AVAILABLE]
[NAME OF COMPANY]
[PHYSICAL STREET ADDRESS - NO P.O. BOX]
[CITY, STATE - NO ZIP CODE]

DEAR **[MR./MRS./MS.] [LAST NAME]:**

Under the authority of Executive Order 12333, dated December 4, 1981, and pursuant to Title 18, United States Code (U.S.C.), Section 2709 (Section 201 of the Electronic Communications Privacy Act of 1986) (as amended, October 26, 2001), you are hereby requested to provide to the Federal Bureau of Investigation (FBI) the name, address, and length of service of **[person or entity] [persons or entities]** to whom the following telephone **[number is or was] [numbers are or were]** registered:

[TELEPHONE NUMBER(S): (000)000-0000]

[RELEVANT TIME PERIOD]: [ON SPECIFIC DATE]

or [FROM [SPECIFIC DATE] to [SPECIFIC DATE]

or [PRESENT]

If the time period noted above is to the "present," that term is intended to request information to the date of the processing of this request. If providing information to the date of processing is not feasible, please provide information to the date of receipt of this request.

In accordance with Title 18, U.S.C., Section 2709(b), I certify that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, and that such an investigation of a United States person is not conducted solely on the basis of activities protected by the First Amendment to the Constitution of the United States.

You are further advised that Title 18, U.S.C., Section 2709(c), prohibits any officer, employee or agent of yours from disclosing to any person that the FBI has sought or obtained access to information or records under these provisions.

You are requested to provide records responsive to this request **[personally to a representative of the [DELIVERING DIVISION]** OR **through use of a delivery service to [OFFICE OF ORIGIN]]** within [xxxx] business days of receipt of this request.

Any questions you have regarding this request should be directed only to the **[[DELIVERING DIVISION]** OR **[OFFICE OF ORIGIN], depending on whether service is personal or through a delivery service]**. Due to security considerations, you should neither send the records through routine mail service nor disclose the substance of this request in any telephone conversation.

Your cooperation in this matter is greatly appreciated.

Sincerely yours,

[ADIC/SAC NAME]
[ASSISTANT DIRECTOR IN CHARGE/
SPECIAL AGENT IN CHARGE]

[DRAFTING DIVISION]
[STREET ADDRESS]
[CITY, STATE, ZIP CODE]
[MONTH, DAY, YEAR]

[MR./MRS./MS.] [COMPLETE NAME OF POC]
[TITLE, IF AVAILABLE]
[NAME OF COMPANY]
[PHYSICAL STREET ADDRESS - NO P.O. BOX]
[CITY, STATE - NO ZIP CODE]

DEAR **[MR./MRS./MS.] [LAST NAME]:**

Under the authority of Executive Order 12333, dated December 4, 1981, and pursuant to Title 18, United States Code (U.S.C.), Section 2709 (Section 201 of the Electronic Communications Privacy Act of 1986) (as amended, October 26, 2001), you are hereby requested to provide to the Federal Bureau of Investigation (FBI) the name, address, length of service, and local and long distance toll billing records associated with the following:

[NAME, IF KNOWN]

[TELEPHONE NUMBER(S) (000)000-0000]:

[RELEVANT TIME PERIOD]: [ON SPECIFIC DATE(S)]

or FROM [SPECIFIC DATE] to [SPECIFIC DATE]

or [PRESENT]

If the time period noted above is to the "present," that term is intended to request information to the date of the processing of this request. If providing information to the date of processing is not feasible, please provide information to the date of receipt of this request.

In accordance with Title 18, U.S.C., Section 2709(b), I certify that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, and that such an investigation of a United States person is not conducted solely on the basis of activities protected by the First Amendment to the Constitution of the United States.

You are further advised that Title 18, U.S.C., Section 2709(c), prohibits any officer, employee or agent of yours from disclosing to any person that the FBI has sought or obtained access to information or records under these provisions.

You are requested to provide records responsive to this request **[personally to a representative of the [DELIVERING DIVISION]** OR **through use of a delivery service to [OFFICE OF ORIGIN]]** within [xxxx] business days of receipt of this request.

Any questions you have regarding this request should be directed only to the **[[DELIVERING DIVISION]** OR **[OFFICE OF ORIGIN], depending on whether service is personal or through a delivery service]**. Due to security considerations, you should neither send the records through routine mail service nor disclose the substance of this request in any telephone conversation.

Your cooperation in this matter is greatly appreciated.

Sincerely yours,

[ADIC/SAC NAME]
[ASSISTANT DIRECTOR IN CHARGE/
SPECIAL AGENT IN CHARGE]

ATTACHMENT

In preparing your response to this National Security Letter, you should determine whether your company maintains the following types of information which may be considered by you to be toll billing records in accordance with Title 18, United States Code, Section 2709:

b2
b7E

[redacted]

We are not requesting, and you should not provide, information pursuant to this request that would disclose the content of any electronic communication as defined in Title 18, United States Code, Section 2510(8).

[DRAFTING DIVISION]
[STREET ADDRESS]
[CITY, STATE, ZIP CODE]
[MONTH, DAY, YEAR]

[MR./MRS./MS.] [COMPLETE NAME OF POC]
[TITLE, IF AVAILABLE]
[NAME OF COMPANY]
[PHYSICAL STREET ADDRESS - NO P.O. BOX]
[CITY, STATE - NO ZIP CODE]

DEAR [MR./MRS./MS.] [LAST NAME]:

Under the authority of Executive Order 12333, dated December 4, 1981, and pursuant to Title 18, United States Code (U.S.C.), Section 2709 (section 201 of the Electronic Communications Privacy Act, as amended, October 26, 2001), you are hereby requested to provide the Federal Bureau of Investigation (FBI) the names, addresses, and length of service and electronic communications transactional records, to include existing transaction/activity logs and all electronic mail (e-mail) header information (not to include message content and/or subject fields), for the below-listed **[e-mail/IP]** address holder(s):

[E-mail/IP ADDRESS or ADDRESSES]

[ON A SPECIFIC DATE]

or [FOR THE PERIOD FROM [SPECIFIC DATE] TO [SPECIFIC DATE]

or [PRESENT]]

If the time period noted above is to the "present," that term is intended to request information to the date of the processing of this request. If providing information to the date of processing is not feasible, please provide information to the date of receipt of this request.

While fulfilling this request, please do not disable, suspend, lock, cancel or interrupt service to the above-described subscriber(s) or accounts. A service interruption or degradation may alert the subscriber(s)/account users(s) that investigative action is being taken. If you are not able to fulfill this request without alerting the subscriber/account user, please contact the requester prior to proceeding.

In accordance with Title 18, U.S.C., Section 2709(b), I certify that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, and that such an investigation of a United States person is not conducted solely on the basis of activities protected by the First Amendment to the Constitution of the United States.

You are further advised that Title 18, U.S.C., Section 2709(c), prohibits any officer, employee or agent of yours from disclosing to any person that the FBI has sought or obtained access to information or records under these provisions.

You are requested to provide records responsive to this request **[personally to a representative of the [DELIVERING DIVISION]** OR **through use of a delivery service to [OFFICE OF ORIGIN]]** within [xxxx] business days of receipt of this request.

Any questions you have regarding this request should be directed only to the **[[DELIVERING DIVISION]** OR **[OFFICE OF ORIGIN],_depending on whether service is personal or through a delivery service]**. Due to security considerations, you should neither send the records through routine mail service nor disclose the substance of this request in any telephone conversation.

Your cooperation in this matter is greatly appreciated.

Sincerely,

[ADIC/SAC NAME]
[ASSISTANT DIRECTOR IN CHARGE/
SPECIAL AGENT IN CHARGE]

ATTACHMENT

In preparing your response to this National Security Letter, you should determine whether your company maintains the following types of information which may be considered by you to be an electronic communication transactional record in accordance with Title 18, United States Code, Section 2709:

b2
b7E

This National Security Letter does not request, and you should not provide, information pursuant to this request that would disclose the content of any electronic communication as defined in Title 18, United States Code, Section 2510(8).