Department of Justice

STATEMENT OF
TODD M. HINNEN
ACTING ASSISTANT ATTORNEY GENERAL FOR NATIONAL SECURITY
DEPARTMENT OF JUSTICE

BEFORE THE
SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY
COMMITTEE ON THE JUDICIARY
UNITED STATES HOUSE OF REPRESENTATIVES

AT A HEARING ENTITLED
"THE PERMANENT PROVISIONS OF THE PATRIOT ACT"

PRESENTED ON
MARCH 30, 2011

Statement of
Todd M. Hinnen
Acting Assistant Attorney General for National Security
Department of Justice

Before the
Subcommittee on Crime, Terrorism, and Homeland Security Committee on the Judiciary
United States House of Representatives

At a Hearing Entitled
"The Permanent Provisions of the PATRIOT Act"

Presented on
March 30, 2011

Chairman Sensenbrenner, Ranking Member Scott, and members of the Subcommittee, thank you for inviting me to testify today. Three weeks ago, I testified before this Subcommittee on the three provisions of the Foreign Intelligence Surveillance Act ("FISA") that were recently reauthorized by Congress but are scheduled to sunset again in May: the "roving" surveillance provision, the "lone wolf" definition, and the "business records" provision. Today I will address other national security investigative authorities enacted or amended as part of the USA PATRIOT Act, focusing in particular on the legal authorities relating to national security letters ("NSLs"). These authorities are not currently scheduled to expire, but I understand the Committee would like me to discuss their use, oversight, and importance to national security. Before I do that, I'd like to provide a brief overview of the investigative tools Congress enacted in the USA PATRIOT Act and why they remain important today.

Investigative Authorities in the USA PATRIOT Act

Nearly ten years ago, shortly after the September 11 attacks, Congress enacted the USA PATRIOT Act, a key purpose of which was "to enhance law enforcement investigatory tools" to protect the country from terrorism. *See* United and Strengthening America by Providing Appropriate Tools Required To Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272, 272 (2001). Title II of the original PATRIOT Act, entitled "enhanced surveillance procedures," contains a number of important amendments to FISA and other laws to make national security investigations more effective and efficient. Of these Title II provisions, 16 were scheduled to expire in 2005, but Congress made 14 of them permanent in the USA PATRIOT Improvement and Reauthorization Act of 2005 while extending the sunsets on the roving surveillance and business records provisions. *See* USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, §§ 102-03, 120 Stat. 192, 194-95 (2006).

The enhancements that were made to our investigative tools in the PATRIOT Act are now fundamental to how we conduct national security investigations. For example, provisions in the PATRIOT Act helped us tear down the so-called FISA "wall" between law enforcement and intelligence. *See* USA PATRIOT Act, sections 203, 218 and 504. The wall had two aspects:

there were limits on intelligence agents' ability to share information they collected using intelligence tools with criminal investigators; and there were limits on the ability of criminal investigators to share information they collected using criminal tools with their colleagues on the intelligence side.

On the intelligence side, the wall was built on the proposition that because FISA required *the* purpose of surveillance to be collection of foreign intelligence,, which was widely interpreted to mean "the primary purpose," the statute itself regulated the nature and scope of interactions between intelligence and law enforcement officials. The PATRIOT Act eliminated the perceived statutory bar on such information sharing, and the FISA Court of Review issued an important decision upholding the Act's clarification that so long as a "significant purpose" of the FISA surveillance is to obtain foreign intelligence, the statute permits a greater degree of interaction between intelligence and law enforcement officials than was previously thought permissible. Other provisions adopted in the PATRIOT Act addressed the other side of the wall. For example, section 203 revised the Wiretap Act and Federal Rule of Criminal Procedure 6(e) to facilitate sharing of Title III and grand jury material involving foreign intelligence or counterintelligence with any Federal law enforcement, intelligence, or national security official to assist them in performing their duties. These were commonsense measures that greatly facilitated our ability to implement broad-based information sharing in the national security arena.

The cumulative result of the elimination of the wall is better cooperation than ever before between the intelligence and law enforcement communities. The National Security Division that I currently head embodies this fundamental change, as criminal prosecutors and intelligence lawyers responsible for implementing FISA are integrated in a single organizational division. The result is not only more effective investigations in which law enforcement and intelligence officials work together to protect Americans, but also more efficient use of these sensitive authorities. National Security Division lawyers work closely with investigators virtually from the outset of an investigation, providing legal advice and oversight as it progresses. The FBI has also reorganized itself to integrate intelligence and law enforcement functions. The results of these changes are seen in cases such as the investigation and arrest in September 2009 of Najibullah Zazi, who plotted to attack the New York City subway system. Intelligence and law enforcement tools were both used and prosecutors and agents worked together to prevent a terrorist attack and then effectively prosecute the case.

Some provisions of the PATRIOT Act were designed to modernize investigative authorities to take account of evolving technologies. For example, section 216 clarified that district courts may authorize pen register and trap and trace devices to be used in criminal investigations to obtain dialing, routing, addressing, or signaling information for electronic communications (*e.g.*, e-mail) in addition to telephonic communications (while prohibiting

collection of content). 18 U.S.C. §§ 3123(a)(1), 3127(3) & (4). Use of pen/trap authority for electronic communications is now routine and a vital part of the investigative tool-kit in criminal cases. The showing that the government must make to obtain a pen/trap order under FISA was also changed in section 214 to bring it into line with the standard applicable in ordinary criminal cases, which requires only that the information sought be relevant to an ongoing criminal investigation. *See* 18 U.S.C. § 3122(b)(2). Before the PATRIOT Act, the government had to show that the facility in question was in communication with a foreign power or agent of a foreign power or an individual engaged in international terrorism or clandestine intelligence activities; now it is sufficient that the information likely to be obtained is "relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities" or is "foreign intelligence information not concerning a United States person." 50 U.S.C. § 1842(c)(2). At the same time, the law precludes an investigation of a United States person based solely upon activities protected by the First Amendment. As revised, the FISA pen register/trap and trace authority is an effective tool that allows investigators operating in the national security arena to gather basic information using the same tools that ordinary criminal investigators have used effectively and without controversy for decades.

Other provisions of the PATRIOT Act were designed to streamline our national security investigations and make them more efficient. For example, section 207, as expanded in 2005 by section 105 of the USA PATRIOT Improvement and Reauthorization Act , extended the time periods for which electronic surveillance and physical searches targeting non-United States persons are authorized under a FISA Court order before a renewal order must be obtained (this time period was later adjusted again by the FISA Amendments Act of 2008). 50 U.S.C. §§ 1805(d)(1), 1824(d)(1). This has allowed the FBI and the National Security Division to focus more of our limited resources on new investigative activity where it is most needed rather than on repeated renewals of FISA applications. Section 216 granted district courts nationwide jurisdiction to authorize pen register and trap and trace devices. 18 U.S.C. § 3123(a)(1). This allows criminal investigators to serve pen register/trap and trace orders on providers anywhere in the country, rather than requiring them to waste valuable time and resources obtaining each order from the district court in the district in which the provider happens to be located.

While I have not catalogued today all of its important reforms, I hope the examples I have provided demonstrate that the tools that are part of the USA PATRIOT Act are critical for national security investigations. The authorities obtained have allowed the Department of Justice and the FBI to more effectively and efficiently achieve their mission of protecting the country from international terrorism and national security threats. We work hard to use these authorities responsibly and in a manner that is consistent with the civil liberties that Americans hold dear, complying with the many safeguards required by statute and developing additional safeguards as a matter of policy and practice. With that brief introduction, I'll address in detail one type of investigative tool that was improved by the PATRIOT Act, although the authority existed long

before the enactment of that statute, and that remains critical to our ability to keep the country safe: national security letters.

The NSL Statutes

A national security letter is effectively an administrative subpoena, issued by a federal agency, requiring the production of certain limited types of information held by third-party custodians. NSLs are used during national security investigations in much the same way as grand jury subpoenas are used during routine criminal investigations. NSLs and grand jury subpoenas allow investigators to acquire the sort of very basic information that can be used as building blocks of an investigation; documents like telephone toll records, and banking and credit records. Unlike grand jury subpoenas, however, NSL authorities are limited to only certain types of records and are found in several distinct statutes, each of which has specific rules governing its use, the types of records that can be obtained, and the nature of the certification that must be provided. And, unlike most grand jury subpoenas, the NSL statutes all contain nondisclosure provisions, which, upon certification from a specified government official, restrict the recipient's right to disclose the NSL. Finally, also unlike grand jury subpoenas, the government must report to Congress specific information regarding its use of NSLs.

It is important to note that the USA PATRIOT Act did not create NSLs; it did, however, change the standard of proof required to issue NSLs. Whereas before the USA PATRIOT Act there had to be specific and articulable facts demonstrating that the information sought pertained to a foreign power or an agent of a foreign power, it is now sufficient that the material sought by an NSL be relevant to a national security investigation. In addition, the USA PATRIOT Act allowed the delegation of NSL approval authority, which, for FBI, had previously been reserved to FBI Headquarters and the three largest field offices, to all FBI field offices, provided that the NSL is approved by an official at the level of Special Agent in Charge ("SAC") or higher. Most of the NSL statutes also expressly require that, if the subject of the investigation is a United States person, it not be based solely on activities protected by the First Amendment. In addition, the Attorney General's Guidelines for Domestic FBI Operations — which also apply to the issuance of NSLs — prohibit the collection, investigation, or maintenance of information on United States persons solely for purposes of monitoring activities protected by the First Amendment or the lawful exercise of other rights secured by the Constitution, and this requirement has been incorporated into FBI policy.

There are five statutes that authorize the issuance of NSLs: the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2709; the Right to Financial Privacy Act ("RFPA"), 12 U.S.C. § 3414; two provisions of the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. §§ 1681u and v; and the National Security Act ("NSA"), 50 U.S.C. § 436. Three of these authorities may be used only by the FBI, and the other two may be used by the FBI and other

agencies (although other agencies collectively issue only a very small number of NSLs). Because the overwhelming majority of NSLs are issued by the FBI, my testimony focuses on the FBI's use of NSLs.

Under ECPA, the FBI may obtain subscriber information, toll billing records, and electronic communication transactional records from a wire or electronic communications service provider, such as a telephone company or an Internet service provider. This is the NSL authority that is used most frequently by the FBI, and each ECPA NSL must include a certification by an authorized FBI employee at the SAC level or above that the records are being sought for an authorized national security investigation. Examples of "electronic communication transactional records" ("ECTRs") that may be obtained by an ECPA NSL are account numbers, physical addresses, subscriber telephone numbers, IP addresses, and other non-content information that is analogous to subscriber information or toll billing records for telephones. Significantly, the FBI *cannot* obtain the content of communications through an ECPA NSL.

The Department is preparing a proposed amendment to the ECPA NSL statute to clarify the obligation of providers to produce ECTRs and has had discussions with staff on both the House and Senate sides related to that issue. Although this term is included in subsection 2709(a) (which describes the provider's duty to produce records), it is absent from subsection 2709(b) (which requires FBI to make a certification in connection with a request for records). This omission has led a small number of providers to conclude that the FBI is not entitled to obtain ECTRs. In contrast, it has led one court to acknowledge the possibility of the opposite extreme, recognizing in dicta that providers may have an obligation to provide the FBI with ECTRs even if there were no certification of relevance. *See Doe v. Gonzales*, 500 F. Supp. 2d 379, 387 n.6 (S.D.N.Y. 2007) ("Section 2709(b) does not make clear whether any certification by the FBI is required with respect to a request for 'electronic communication transactional records.'"). While we believe the current law requires the production of ECTRs, and that the certification requirement in subsection 2709(b) applies as well, we expect to propose an amendment to eliminate this source of confusion in the statutory text.

Under RFPA, the FBI has the authority to issue NSLs for the financial records of a person or entity from various types of financial institutions, such as banks, credit unions, and credit card companies. RFPA NSLs are commonly used in connection with investigations of potential terrorist financing. Again, each RFPA NSL must include a certification by an authorized FBI employee at the SAC level or above that the records are being sought for an authorized national security investigation. RFPA also allows other agencies to issue NSLs.

Under provisions of FCRA, the FBI has the authority to issue three different, but related, types of NSLs to credit reporting agencies: an NSL pursuant to 15 U.S.C. § 1681u(a) for the names of financial institutions with which the subject has or has had an account; an NSL

pursuant to 15 U.S.C. § 1681u(b) for consumer identifying information (name, address, former addresses, employment, and former employment); and an NSL pursuant to 15 U.S.C. § 1681v for a full credit report. This last one may be used only in international terrorism cases, as opposed to any national security investigation.

Finally, any authorized investigative agency has the authority to issue NSLs pursuant to the National Security Act ("NSA") in the course of investigations of improper disclosure of classified information by government employees. 50 U.S.C. § 436(a)(1)-(2). The standards for issuance of National Security Act NSLs are significantly different than the others. The records sought must pertain to a person who is or was an Executive Branch employee and who provided consent to the government to access his financial records, consumer reports, and travel information as a condition of his access to classified information. Moreover, there must be reasonable grounds to believe that the person is or may be disclosing classified information in an unauthorized manner, has incurred excessive indebtedness or acquired unexplained affluence, or had the capability and opportunity to disclose classified information known to have been lost or compromised. National Security Act NSLs may be issued to financial institutions, consumer credit agencies, and commercial entities with travel information, but must be approved at the Assistant Secretary or Assistant Director level or above. The FBI has not used this authority to date.

As a matter of procedure under FBI policy, an FBI employee seeking an NSL must prepare a document (an electronic communication, or "EC") in which the employee lays out the factual predicate for the request. The factual recitation must be sufficiently detailed so that the approving official can determine that the material sought is relevant to an authorized national security investigation. Additionally, it needs to provide enough information concerning the underlying investigation that reviewing officials can confirm that the investigation is adequately predicated and, if concerning a United States person, is not based solely on the exercise of First Amendment rights.

I believe the current standards for issuance of an NSL are appropriate. In a traditional criminal case, a grand jury subpoena may be issued "merely on suspicion that the law is being violated, or even just because [the grand jury] wants assurance that it is not" being violated. *United States v. R. Enterprises*, 498 U.S. 292, 297 (1991). Imposing a higher evidentiary standard on NSLs, as was the case before the reforms of the USA PATRIOT Act, would significantly impair the effectiveness of this important investigative tool. This is true particularly because NSLs are often used at the outset of an investigation when additional facts concerning the subject of the investigation may not be available and when basic information is needed in order to be able to move an investigation forward.

Challenging NSL Nondisclosure

As noted above, all of the NSL statutes contain provisions barring the recipients from disclosing the NSL (except to an attorney or other person whose assistance is required to comply) based upon a certification that nondisclosure is necessary. The FBI (as well as other agencies issuing NSLs) must make an individualized determination for every NSL it issues whether there is a need for secrecy based on a danger to national security or interference with an investigation that might result from disclosure. Generally the need for secrecy derives from a desire not to reveal prematurely the existence of the investigation to its targets. If the need for secrecy is certified, the NSL may forbid the recipient from disclosing it unless and until the recipient obtains a judicial order for relief.

In *Doe v. Mukasey*, 549 F.3d 861 (2d Cir. 2008), the recipient of an ECPA NSL challenged the constitutionality of the nondisclosure requirement in court. The United States Court of Appeals for the Second Circuit found the statute unconstitutional under the First Amendment because it imposes a burden on the recipient to initiate litigation in order to protect his free speech interests, but observed that the government could cure this problem with a "reciprocal notice" approach: "The Government could inform each NSL recipient that it should give the Government prompt notice, perhaps within ten days, in the event that the recipient wishes to contest the nondisclosure requirement. Upon receipt of such notice, the Government could be accorded a limited time, perhaps 30 days, to initiate a judicial review proceeding to maintain the nondisclosure requirement, and the proceeding would have to be concluded within a prescribed time, perhaps 60 days." *Id.* at 879. Thus the court struck down the nondisclosure provisions "only to the extent that they fail to provide for Government-initiated judicial review," and stated that the government "can respond to this partial invalidation ruling by using the suggested reciprocal notice procedure," which if implemented would allow the nondisclosure provisions to "survive First Amendment challenge." *Id.* at 884. The FBI promptly implemented the reciprocal notice procedure as suggested by the court for all types of NSLs. The *Doe* court also struck down a separate statutory requirement that the government's certification, which triggers the nondisclosure requirement, must be treated as "conclusive" absent a finding of bad faith; the court required "some demonstration" from the government to allow for meaningful judicial review on the merits. *Id.* at 882.

Legislation now pending in the Senate to reauthorize the three expiring FISA authorities would essentially codify the reciprocal notice practice for NSL nondisclosure challenges and eliminate the conclusive presumption, thus rendering the non-disclosure provisions of the NSL statutes facially constitutional. *See* S.193, "USA PATRIOT Act Sunset Extension Act of 2011." In place of the conclusive presumption afforded the government's determination on the need for secrecy, under the Senate bill, the court would be required to give "substantial weight" to the government's determination that disclosure of the NSL would endanger national security or harm

an investigation. The bill would also require the government to notify the recipient of an order who has objected to nondisclosure if and when the need for government secrecy no longer exists. We believe these procedures are constitutionally and operationally sound and give the government and the recipient a fair chance to litigate the nondisclosure requirements.

Since shortly after the *Doe* decision, the FBI has given all NSL recipients the option of notifying the FBI if they wish to be released from their secrecy obligation. Only one recipient of an NSL has objected to nondisclosure; the issue was resolved without the necessity of litigation.

The NSL Subsystem

In 2007, the Department of Justice Office of the Inspector General ("OIG") issued a report that was critical of the FBI's use of NSL authorities. For example, the report found that NSLs had been issued when the investigative authority to conduct the underlying investigation had lapsed; that telephone billing and e-mail subscriber records had been obtained concerning the wrong individuals; that NSLs were issued citing the wrong statutory authorities; that full credit reports had been obtained in counterintelligence investigations, which the relevant NSL statute does not permit; and that NSLs were issued out of "control files" rather than from "investigative files" in violation of FBI policy. *See* Department of Justice Office of Inspector General Report, "A Review of the Federal Bureau of Investigation's Use of National Security Letters," at 66-67 (March 2007). However, as the Inspector General testified in 2007, "in most -- but not all of the cases we examined in this review, the FBI was seeking information that it could have obtained properly through national security letters if it had followed applicable statutes, guidelines, and internal policies." *See* Statement of Glenn A. Fine, Inspector General, U.S. Department of Justice, before the House Judiciary Committee concerning the FBI's Use of National Security Letters and Section 215 Requests for Business Records," (March 20, 2007) at 4. The Inspector General also found that FBI agents had not intentionally sought to misuse NSLs but that the misuses were the product of "mistakes, carelessness, confusion, sloppiness, lack of training, lack of adequate guidance, and lack of adequate oversight." *Id.*

In the wake of this report, the FBI developed an automated system – the NSL subsystem – under which NSLs would be issued in order to control for and prevent most non-substantive errors. The NSL subsystem was created to be a part of the existing, highly successful FISA Management System; it functions as a workflow tool that automates much of the work in preparing NSLs and their associated paperwork. It is designed to require the user to enter certain data before the workflow can proceed and requires specific reviews and approvals before the request for the NSL can proceed. Through this process, the FBI can electronically ensure that applicable legal and administrative requirements are met and that required reporting data are accurately collected.

For example, by requiring the user to identify the investigative file from which the NSL is to be issued, the system ensures that NSLs are not requested out of administrative or control files. In addition, the subsystem automatically verifies the status of the case to ensure that the investigation is still open at the time the NSL is drafted. It also automatically populates the NSL with appropriate statutory language, validates the case file through the FBI's case file system to ensure that the case is open and a proper sub-file has been identified, and ensures that the underlying investigation has not lapsed. Thus, for instance, the system would prevent a user from relying on the FCRA NSL provision, 15 U.S.C. 1681v – which applies only in terrorism investigations – to issue an NSL in a counterintelligence investigation. The system requires the user to identify separately the target of the investigative file and, if it is a different person, the identity of the person about whom records are being obtained through the requested NSL. This allows the FBI to tabulate more accurately the number of different persons about whom data is gathered using NSLs – one of the data points on which the government is required to report to Congress. The system also requires that specific data elements be entered before the process can continue, such as requiring that the target's status as a United States Person ("USPER") or non-USPER be entered, or requiring that an FBI lawyer approve the legal sufficiency of the grounds for which the NSL is sought. The system does not permit requests containing logically inconsistent answers to proceed.

The NSL subsystem was designed so that the FBI employee requesting an NSL need enter data once and the subsystem automatically populates all subsequent places where those data are needed. Among other things, this eliminated one particular type of transcription error that gave rise in the past to unauthorized collections (*e.g.*, the relevant telephone number on which records were requested in the authorizing EC was 202-333-1234, but due to a typographical error in the NSL served on the telephone company, the FBI asked for records relating to 202-333-1243). In addition, requesters are required to provide a narrative statement explaining the factual basis for the determination that the information being sought is relevant to an appropriately predicated national security investigation, and the basis for a determination that the NSL should include a non-disclosure provision, if such a provision is included.

The NSL subsystem also ensures that both the NSL and the EC supporting issuance of the NSL are reviewed and approved in accordance with FBI policy, which now mandates review and approval by an FBI attorney. (Prior to the 2007 OIG report, legal review of NSLs had been recommended but not required; in addition, the exact scope of the lawyer's review obligation had not been defined). In addition, only an FBI employee who is statutorily authorized to do so can authorize issuance of the NSL in the subsystem. Once approved in the subsystem, the various documents are automatically uploaded into the FBI's Automated Case Support System ("ACS").

Finally, this subsystem has a comprehensive Congressional reporting capability. Since its deployment, FBI policy has required all NSLs to be created using the NSL subsystem, with

only a few very narrow exceptions (*e.g.*, very sensitive investigations such as espionage investigations). The system has increased the accuracy of NSL reporting, reduced drafting errors, and has ensured all required levels of approval have been obtained. By FBI policy, NSLs that are created outside of the NSL subsystem must be reported to the Office of the General Counsel ("OGC") and the information required for Congressional reporting is manually entered into the system.

Based on several audits of the subsystem by the FBI's Inspection Division, the Department has concluded that the subsystem has significantly improved the FBI's compliance with the NSL statute and has reduced errors in the production of NSLs to a very low rate. It also has increased the accuracy of NSL reporting.

FBI/DOJ Oversight of NSLs

Following the 2007 OIG Report regarding NSLs, the FBI also took a hard look at all of its policies regarding NSLs and the communication of those policies to FBI employees. In addition to developing and deploying the NSL subsystem, the FBI tightened policies and procedures that existed and ensured that they were all put into a single comprehensive document that was disseminated to the field. That document required legal reviews of all NSLs, required retention of signed copies of NSLs and ECs supporting the NSLs in the investigative file, and required a review of information received in response to an NSL to ensure there had been no "overproduction" of information. Since December 2008, all of those rules have been available in the FBI's Domestic Investigations and Operations Guide ("DIOG"), of which employees have copies and which also is available to all employees on their FBI computers.

In addition, since 2008, the FBI's Inspection Division has conducted a number of NSL audits. The Inspection Division audit is a focused review of the use of NSLs in an effort to assess the FBI's compliance with all applicable policies, statutes, and guidelines with respect to the issuance of NSLs and the handling of NSL results, to determine the efficacy of corrective actions taken subsequent to their prior audits, and to propose additional corrective action as appropriate. The Inspection Division audit reviews every NSL that is created outside of the NSL subsystem. For NSLs prepared within the subsystem, the Inspection Division audits a sample. Each Inspection Division audit thus far has shown minimal non-compliance, with the most recent audits for 2008 and 2009 showing only about 0.7% of reviewed NSLs having any compliance issues.

Also following the OIG's 2007 NSL review, the FBI established a compliance office, modeled on those established by publicly-traded companies, to look critically at areas of legal risk to ensure that policies, procedures, and training were designed and executed in a way that

would maximize the likelihood of full legal compliance. That office, the Office of Integrity and Compliance ("OIC"), is focused on NSLs, as well as other areas of legal risk to the FBI.

The FBI's OGC has conducted extensive NSL training both at FBI Headquarters and in field offices. In addition, an online training course is required for all employees involved in drafting, reviewing, and approving NSLs.

Finally, the Department of Justice, National Security Division, and the FBI's OGC conduct oversight of FBI field offices each year through National Security Reviews ("NSRs"). The NSR teams typically review between 15-20 field offices per year. During those reviews, among other compliance issues, attorneys conduct comprehensive reviews of the field office's use of NSLs, including compliance with the applicable laws and policies.

For each national security investigation reviewed, the NSR teams examine all aspects of NSL use in the investigation. For each NSL selected, the NSR teams examine the authorizing EC, the NSL itself, and the subsequent results. For example, among the items considered during the review, the teams analyze the NSL's authorizing EC to ensure that there is a sufficient nexus between the records sought and the investigation. In so doing, the teams can verify not only that the FBI has established the relevancy of the request to the investigation, as required by the authorizing NSL statutes, but also documented that nexus so that the approving officials have enough information to make an informed decision regarding authorization of the NSL.

The NSR teams also examine the NSL to determine the scope of the request and carefully review the results supplied in response. In this manner, the NSR teams are able to verify whether the FBI is properly handling those instances when material is provided that exceeds the scope of an NSL. Although over-productions are the result of third-party action, it is the FBI's responsibility to manage correctly the disposition of such information. This includes promptly identifying the over-production, as well as ensuring that over-produced material is not used in furtherance of an investigation or uploaded into FBI databases.

It is noteworthy that, even as of 2008, the Office of Inspector General concluded that "since the issuance of our March 2007 report, the FBI and the Department have made significant progress in implementing the recommendations from that report and in adopting other corrective actions to address serious problems we identified in the use of national security letters." *See* Department of Justice Office of Inspector General Report, "A Review of the FBI's Use of National Security Letters: Assessment of NSL Usage in 2006" (March 2008). Since that time, the FBI and DOJ reviews described above have found that NSLs are being properly issued in the overwhelming majority of cases. At the conclusion of each NSR, the field office receives an oral out-briefing detailing the results of the review, including its handling of NSLs, and providing

recommendations regarding any areas found to be deficient. This is followed up by a formal written report.

NSL Procedures

Last year, the Attorney General approved new procedures for FBI's collection, use, and storage of information obtained from NSLs. The purpose of these procedures is to improve adherence to the NSL statutes and provide additional privacy safeguards for NSL-obtained information without impeding the FBI's operational and technical mission requirements. These procedures are designed to interrelate with the DIOG mentioned above, which in turn implements the Attorney General's Guidelines for Domestic FBI Operations, also mentioned above. Department officials have briefed Congress, including the House and Senate Judiciary Committees, on these new procedures.

As set forth in the new procedures, FBI employees must review all information produced in response to NSLs seeking financial records to ensure that information that (a) is not responsive to the NSL or (b) has no investigative value is not entered into the electronic case file. If the information is responsive to the NSL ***and*** has potential investigative value, it may be uploaded into the Automated Case Support System ("ACS") or other FBI databases. NSL-derived information may, however, be entered temporarily into local electronic files on desktop computers for initial analysis to determine whether it is responsive and has investigative value. Any non-responsive information must be sequestered with the chief division counsel ("CDC") or the National Security Law Branch ("NSLB") for proper handling (*i.e.*, either destruction or return to the party from which they were requested), and the NSLB must be notified of the over-production, in accordance with established procedures.

As the FBI develops technology to assist in the analysis of financial data, so that the FBI can draw important investigative links between disparate data, all data that are responsive to NSLs (regardless of whether it is assessed to have immediate investigative value) may be entered into a separate, secure database with effective access controls, an established access policy, and an effective audit capability to monitor compliance. The access policy must ensure that NSL data in the separate data base (*i.e.*, data that were responsive to NSL requests but did not have apparent investigative value at the time they were received) are not retrieved and uploaded into ACS unless and until their investigative value is established through an authorized search of the separate database. Information that is not responsive to the NSL request may not be uploaded into any FBI database and must either be destroyed or returned to the provider.

The Value of NSLs

I would like to conclude my remarks by emphasizing how important NSLs are to our national security. NSLs are an indispensable investigative tool, and have often been described as the "building blocks" of national security investigations. NSLs contribute significantly to the FBI's ability to carry out its national security responsibilities by directly supporting its counterterrorism, counterintelligence, and intelligence missions.

As reported in the Department's last annual report on NSL usage, excluding requests for subscriber information (*i.e.*, an NSL issued to ascertain the subscriber associated with a particular telephone or email address), in 2009, the FBI made 14,788 NSL requests for information concerning 6,114 different United States persons. In 2008, the FBI made 24,744 NSL requests (excluding requests for subscriber information) pertaining to 7,225 United States persons. These numbers reflect the importance of these tools to the FBI, but also reflect the fact that the FBI uses NSLs to obtain information regarding a very small portion of the American population.

NSLs are issued by the FBI in national security cases for a variety of investigative reasons. They are used in counterintelligence cases in which individuals are suspected of attempting to steal our nation's secrets, including espionage cases. They are used extensively in terrorism cases to help correctly identify international terrorists and thwart future attacks in the United States. As an investigative tool, NSLs are integral to determining whether, how, and by whom our nation is being put at risk. So, while I cannot discuss specific investigative techniques that were used in specific investigations, NSLs were used in most cases, if not every major case, in which the FBI has disrupted terrorist plots against the homeland or identified spies working to obtain classified United States Government information. These tools have helped keep our nation safe, while safeguarding the civil liberties of all Americans.