Testimony of Lisa Graves
Deputy Director
Center for National Security Studies

"Unchecked National Security Letter Powers and Our Civil Liberties"

Before the House Permanent Select Committee on Intelligence
United States House of Representatives
March 28, 2007

On behalf of the Center for National Security Studies and my partner there, Director Kate Martin, I thank Chairman Reyes and the Ranking Member for the invitation to testify today about the FBI's severe misuses of the controversial National Security Letter (NSL) powers.

What is CNSS? The Center is a civil liberties organization, which for more than 30 years has worked to ensure that civil liberties and human rights are not eroded in the name of national security. The Center is guided by the conviction that our national security must and can be protected without undermining the fundamental rights of individuals guaranteed by the Bill of Rights. In our work on matters ranging from national security surveillance to intelligence oversight, we begin with the premise that both national security interests and civil liberties protections must be taken seriously and, that by doing so, solutions to apparent conflicts can often be found without compromising either. The Center has worked on issues concerning national security letters both before and since enactment of the Patriot Act, and we are pleased to testify before this Committee again and meet with the new Chairman, Ranking Member Hoekstra and the other distinguished Members of this Committee charged with the oversight of U.S. intelligence-gathering operations.

NSL Implementation Earns an "F." This Committee is responsible for helping to ensure that any powers used by the Executive Branch are focused, effective and protect our civil liberties. The NSL powers fail that test. Their focus is too diffuse. The anecdotal evidence of their effectiveness is disproportionately small compared with the extent of their use and the invasion of privacy they represent. Civil liberties have not been adequately protected. The implementation of the requirements for using these intrusive powers was sloppy. The weak procedures intended to provide some protection were circumvented hundreds of times and this happened at FBI headquarters. The Inspector General's audit shows empirically that these intrusive NSL powers have been seriously misused. This is a substantial failure. An "F." And that is the grade according to the FBI's General Counsel.[1]

---

1 Testimony of FBI General Counsel Valerie Caproni before the House Judiciary Committee on March 20, 2007. Ms. Caproni volunteered this assessment in response to a question by Congressman Cohen, stating "we got an F report card when we're just not used to that. So we've had a lot of discussions about this. And one concern is, are we -- you know, most of the agents grew up, the agents my age in the FBI, all grew up as criminal agents in a system which is transparent, which, if they mess up in the course of an investigation, they're going to be cross-examined, they're going to have a federal district judge yelling at them. The national security side occurs largely without that level of transparency." CQ HJC Transcript of March 20, 2007 at p. 34.

There is no doubt the Bureau has faced many pressures since September 11th but, as the IG has noted, that does not excuse these failures.[2] I know from working at the highest levels of the Justice Department on firearms and immigration policies, among other issues, that there are many devoted civil servants as well as agents and lawyers at the Bureau who are dedicated and professional. But we must be a nation of laws, not left to the good intentions of particular men or women whom we trust. The Bureau needs clear rules and independent oversight that is not optional. More internal rules simply won't fix the severe flaws in these NSL powers. The failures exposed by the IG warrant real, external checks.

The administration has had no choice but to acknowledge these failures. They insist the only problem was one of implementation. But the bigger problem is that the NSL power allows too much sensitive information to be gathered based on too little predication on too many Americans who have done nothing wrong, and to keep that private information for too long.

The Audit Shows More Scrutiny of NSL Powers Is Greatly Needed. The IG report raises many red flags that warrant intense scrutiny by Congress and the American people. Today, I will highlight two of the major concerns calling for additional public hearings and reform. First, the rules for gathering Americans' sensitive records are too loose. Second, the financial, Internet and phone records obtained are kept for too long, even if there is no reasonable basis to believe an individual is doing anything wrong. The situation created by these intrusive powers is very troubling because, as the IG observed in late 2006:

> [W]hen Congress lowered the evidentiary standard for issuing National Security Letters . . . it authorized the FBI to collect information . . . on persons who are not subjects of FBI investigations. This means that the FBI—and other law enforcement or Intelligence Community agencies with access to FBI databases—is able to review and store information about American citizens and others in the United States who are not subjects of FBI foreign counterintelligence investigations and about whom the FBI has no individualized suspicion of illegal activity.[3]

<u>The NSL Rules for Gathering Sensitive Records Are Too Loose.</u>
The IG expressed concern that NSLs can be used to demand sensitive records on people "two or three steps removed" from the subject of an investigation, without any required determination of suspicious activities by such people.[4] This raises serious civil liberties concerns. If the conventional wisdom is that every person is separated from any other person by only six degrees of separation, this puts us half the way there.

It Can Sweep In People With Two or Three Degrees of Separation. Suppose you have a suspected terrorist who is the subject of a full investigation, meaning his phone conversations can be legitimately wiretapped and home searched with court orders. The

---

2 *Id.* at p. 8. Mr. Glenn Fine added that the FBI's failures "were serious and unacceptable."
3 Department of Justice, FY 2006 Performance and Accountability Report, at p. IV-32.
4 Office of the Inspector General, A Review of the Federal Bureau of Investigation's Use of National Security Letters, March 2007, at p. xlii of the unclassified Executive Summary (hereinafter "NSL Audit"). *See also id.* at p. 108.

FBI can demand all his past phone records with an NSL or get a pen register to monitor his calls contemporaneously with a court order. The FBI then has a list of everyone he calls or who calls him—that's one step removed. This list could include the numbers of the pizza delivery business, the dry cleaner or his lawyer as well as any actual co-conspirators. As the IG indicated, however, there is nothing in the expansive NSL authorities to prevent records from being gathered on people two or three steps removed. Could they get all the lawyer's financial records or map all of her phone calls? That's one or two steps removed. Suppose the lawyer calls a journalist or even contacts Congress—can the phone records and financial records of such third parties be gathered and retained? That could be only two or three steps removed from the subject or target of an investigation. We do not know how often this has happened because as thorough as the audit was it did not drill down into particular investigations to audit them for this or check who is in the FBI's Investigative Data Warehouse, which has over 560,000,000 records.[5] It is noteworthy, however, that there are public reports that Bureau employees have complained about the amount of time wasted time following up on "leads" that lack any suspicious connections or actions.[6]

The Standard for Data Collection Is Too Low. What would prevent anyone's full credit file, for example, from being gathered? Post-Patriot, no court approval is required for such information. In general, NSL demands can be signed by an FBI Special Agent-in-Charge (SAC) in the field or a designee at FBI headquarters based on a statement that records are sought for an authorized investigation to protect against international terrorism.[7] And, the requirement that the records "pertain" to a foreign power, suspected agent of a foreign power or a US person conspiring with them was eliminated through the Patriot Act changes. In fact, any agency authorized to investigate international terrorism is permitted to obtain full consumer credit files, not just the FBI[8]—although there has been no full audit of which agencies have used this power and to what extent. Although there are some technical differences between the five NSL statutes, the common denominator is that the demand is allowed based on the self-certification by Executive Branch agents and there is no requirement that the records be about a suspected terrorist or his co-conspirators or even that there be specific facts connecting the records of others sought to a suspected agent. The main threshold is that the records be relevant to an authorized investigation.

These Low Standards Were Breached, Repeatedly. As the IG found, however, even these minimal procedures were regularly not followed. FBI employees not approved to issue NSLs did so, and units at FBI headquarters issued NSLs that were not tied to an authorized investigation.[9] Without the need to get court approval and with the cloak of secrecy, the weak limitations in the NSL statutes were violated repeatedly.[10]

---

5 NSL Audit at p. 30.

6 Barton Gellman, In Hunt for Terrorists, Bureau Examines Records of Ordinary Americans, Washington Post, November 6, 2005, at p. A01.

7 Pub. L. No. 107-56, § 505, 115 Stat. 365-66 (2001). The five NSL powers are in the following statutes: Section 1114(a)(5) of the Right to Financial Privacy Act (12 U.S.C. 3414(a)(5)); sections 626 and 627 of the Fair Credit Reporting Act (15 U.S.C. 1681u, 1681v); section 2709 of title 18 of the United States Code; and section 802 of the National Security Act (50 U.S.C. 436).

8 Pub. L. No. 107-56, § 358(g), 115 Stat. 327 (2001) (modifying 15 U.S.C. 1681b).

9 *See, e.g.,* NSL Audit at p. 30; March 20, 2007 HJC transcript at p. 8.

10 *See, e.g.,* March 20, 2007 HJC transcript at p. 34.

For example, for over five years, an unknown number of NSLs have been issued based on a perfunctory assertion of relevance, without a meaningful explanation of why the records sought were relevant to the investigation.[11] Similarly, NSLs continue to recite the mantra that the records sought are not based solely on protected First Amendment activities, but one cannot know if this rote recitation is correct when there are no facts to back it up showing the grounds for seeking such records. And the IG did not verify each of the nearly 150,000 NSL demands made between 2003 and 2005 or the NSLs issued the first two years or last year. (As the IG made clear, these figures are understated due to the FBI's poor record keeping.) The small sample audited by the IG, along with the improper "exigent" letters and NSLs that were not issued from opened investigation files, establish that important facts were routinely missing from NSLs.

The Renaming of Preliminary Inquiries Lowered the Threshold Further. We cannot take much refuge in the recent announcement that a full statement of facts will now be required, because the threshold for an investigation remains so low. Although the requisite prediction for Foreign Intelligence (FI) investigations of international terrorism is classified, we know that the counter-part Guidelines for Domestic Security/Terrorism Intelligence investigations without an established foreign nexus were weakened under Attorney General Ashcroft. At the time the Patriot Act amended the NSL powers, the unclassified Guidelines required a headquarters finding of "predication" that there was a "reasonable indication" (not probable cause) of violent acts or the planning of such criminal or terrorist acts, and that predication had to be renewed every six months. Ashcroft changed the rules to decentralize opening of investigatory files with less frequent review, and he redefined "preliminary inquiries" to be preliminary "investigations."[12] This allows a large group of agents to open "investigations" on the predicate that there is a "possibility" of terrorist acts without there being a reasonable indication such violence is being planned.

The IG found almost half of all NSLs were issued in preliminary investigations.[13] Notably, Director Mueller has stated that "there is no particular standard of proof" for preliminary investigations and they can be opened based on an "anonymous allegation."[14] Thus, the

---

11 *See* NSL Audit, pp. 112-114.

12 *See, e.g.,* description of investigations at http://www.disastercenter.com/DoJ/Introduction.htm.

13 NSL Audit, p. xxi.

14 Testimony of FBI Director Robert Mueller before the Senate Select Committee on Intelligence on April 27, 2005. These statements in response to questions by Senator Wyden appear in CQ's SSCI Transcript on p. 126. At a related hearing on May 24, 2005, the FBI sought to expand the NSL powers to allow "administrative subpoena" power for any document sought in a terrorism investigation. When asked by Senator Hatch about "the panoply of protections" that would safeguard Americans' civil liberties from abuse of such powers, the General Counsel noted that "There are lots of checks," the first check being that such demands would have to be approved by a Special Agent-in-Charge, subject to review by attorney, and the second that businesses receiving the demand could move to quash it—the very same "controls" noted for NSLs, which failed. *Id.* at pp. 153 and 146; *see also* Testimony of Matthew Berry, Office of Legal Counsel, U.S. Department of Justice, before the Subcommittee on Crime, Terrorism, and Homeland Security of the House Judiciary Committee, May 26, 2005, at p. 46 of the electronic transcript available through the GPO (stating similarly that "there is a process in place at the FBI with multiple layers of review before an NSL is issued"). These are just a few samples of many such statements from the administration about the care and protectiveness of internal controls at FBI for NSLs.

statutory requirement that records demanded with an NSL must be relevant to an "authorized" investigation provides very little protection for civil liberties. Could an unverified, anonymous allegation regarding terrorism about anyone in this room count as a predicate to open a preliminary investigation and conduct a fishing expedition into one's financial records, credit report, phone bills, or internet transactions? The NSL statutes do not appear to provide much protection against this happening through false allegations of a connection to international terrorism or through guilt by association.

NSLs Were Issued Without Ties to Investigatory Files. And yet even the very limited standard of being relevant to an authorized investigation was violated, and at FBI Headquarters no less. In one set of violations over several years, the IG found that NSLs were issued from "control" files, which by definition lack even the minimal predication for a preliminary inquiry, let alone a full investigation.[15] According to the IG, approximately 300 NSLs involving an unverified number of US citizens or residents were issued for phone records, subscriber information or e-mail transactions.[16] Near the end of the IG's audit, the FBI purportedly "solved" this problem by opening a generic, or an "umbrella," investigation for this classified special project of the Counterterrorism Division.[17]

NSLs Were Circumvented with Exigent Requests, Thousands of Times. In another major set of violations also covered after the fact by "umbrella" investigations,[18] the FBI issued over 700 demands for records from telecomm companies on over 3,000 people without providing an NSL before hand or often even after information was gathered.[19] In these 3,000 violations of the rules, the FBI circumvented the minimal requirements of the NSL statutes, through what they called an "exigent letter," without proof of an emergency regarding death or serious injury to a person (which is the standard for the emergency provision giving electronic communications providers safe harbor for certain disclosures).[20] The FBI also entered into contracts with AT&T, MCI, and Verizon for virtually real-time access to subscriber data without proper documentation.[21] The IG was unable to substantiate the factual or legal predicates for many of these demands.[22] In addition, in these examples and across the FBI, the IG noted that agents did not routinely keep copies of signed NSLs or related correspondence, often did not indicate whether the persons whose records were obtained were citizens or residents, and routinely did not track whether they were subjects or targets of an investigation.[23]

---

15 NSL Audit at p. xxxv.
16 *Id.* at. p. 98.
17 *Id.* at p. 99.
18 *Id.* at pp. 93-94. *See generally id.* at 86-97.
19 *Id.* at pp. 90-91.
20 *Id.* at pp. 94-99 (discussing the conflict between the practice and the emergency statute, 18 U.S.C. 2702(c)(4)).
21 March 20, 2007 HJC transcript at p. 37. The General Counsel noted that MCI and Verizon have since merged. (The names of the contracting telecommunications companies do not appear in the unclassified audit report but were disclosed by the General Counsel at the HJC hearing.)
22 NSL Audit at p. 91 (stating that FBI was "unable to provide reliable documentation to substantiate" that the demands were authorized as claimed in the exigent letters).
23 *Id.* at pp. xx, 118. and 124

Sensitive Information Obtained through NSLs Is Kept Too Long—for 20+ Years. After more than five years and far more than 100,000 demands for information, we are now told that the Director of National Intelligence is looking into the issue of whether it is appropriate to retain such information on people who have done nothing wrong or about whom there is no reasonable indication of wrongdoing.[24] It has been reported in a number of papers that the government 's policy is to retain information obtained in terrorism investigations indefinitely even if the person is cleared because it might someday be useful. The General Counsel indicated that NSL disclosures are kept at least 20 years.[25]

Information Kept Even If the Person Is "Cleared" or the Case Is "Closed." This situation would not be so troubling if the information kept for decades were information about suspected agents of foreign powers, like al Qaeda, or US persons conspiring with them. However, the IG expressed concern that there is "no purging of information regardless of the outcome of the investigation."[26] The IG noted that FBI agents say NSLs are very useful in checking out leads and "eliminating concerns" about people or "closing" preliminary investigations,[27] but he flagged the fact that telephone, internet, banking, credit or financial information obtained in any authorized investigation is "indefinitely retained."[28] He also noted that such information is retrievable by thousands of federal government employees.[29] This is extremely troubling from a civil liberties standpoint.

NSLs Can Expose the Private Transactions of Daily Life. It is especially troubling, however, when one realizes that without any individualized suspicion of wrongdoing a very detailed dossier on an individual can be created through these secret powers. The NSL powers allow access not just to information such as who is associated with what telephone number or e-mail account, but also the numbers and names of everyone you call or who calls you and everyone you correspond with by e-mail as well as every website you visit. It allows access to top-line credit bureau information, such as your address, social security number, date of birth, and employer, as well as the numbers of all of your past and present credit accounts, from Victoria's Secret to Visa. With NSLs, the FBI can learn of virtually everything you have purchased with your debit or credit card and can even learn the pin number that allows access to your account. And a change to NSLs added by the Intelligence Authorization for FY 2004 allows access to any record—whether truly financial or not—held by any "financial institution," which was redefined to include insurance companies, real estate closing firms, jewelers, and even the U.S. Postal Service.[30] The

---

24 March 20, 2007 HJC transcript at p. 20.
25 *Id.*
26 NSL Audit at p. xlii.
27 *Id.* at p. 46.
28 *Id.* at p. xlii.
29 *Id.; see also id.* at pp. 28-30.
30 Pub. L. No. 108-177, § 374, 117 Stat. 2628 (2004) (sweeping in records of: (A) an insured bank; (B) a commercial bank or trust company; (C) a private banker; (D) an agency or branch of a foreign bank in the United States; (E) any credit union; (F) a thrift institution; (G) a broker or dealer registered with the Securities and Exchange Commission; (H) a broker or dealer in securities or commodities; (I) an investment banker or company; (J) a currency exchange; (K) an issuer or redeemer of travelers' checks, checks, or money orders; (L) an operator of a credit card system; (M) an insurance company; (N) a dealer in precious metals, stones, or jewels; (O) a pawnbroker; (P) a loan or finance company; (Q) a travel agency; (R) a licensed sender of money or any other

sum of this electronic footprint sweeps up most of the transactions of your daily life, going back many years or perhaps going forward, even if you have not done anything wrong.

A Half-Billion Records Are in the FBI's Data Warehouse. According to the IG, the data obtained through NSLs is input into FBI computer databases and is downloaded routinely into the Investigative Data Warehouse.[31] To date, the FBI's Data Warehouse has over a half billion records.[32] As the IG noted, electronic files includes what is known as "open source" information,[33] which used to mean basically information that could be read in the newspaper or on the Internet but which now includes information government agents can buy about citizens and residents, without even issuing an NSL. The Data Warehouse also includes over 70 million Bank Secrecy Act records, including information based on the approximately 100,000 "suspicious activity reports" filed by banks about their customers, as of two years ago.[34] According to numerous press accounts, SARs and other Patriot Act domestic requirements have resulted in accounts being flagged for activities as innocent as paying off one's credit debt, which has led to anger and frustration with the unexamined consequences of Title III of the Patriot Act on both the right and the left. The combined effect of all of these changes for American civil liberties has yet to be fully examined.

Past Privacy Assurances Have Not Stopped the Creation of a Massive Database. It is unclear how many American citizens and residents have had their private information added to this Data Warehouse, which has more records than there are people living in the US, and surely has exponentially more records than the number of suspected terrorists. What is clear is that past assurances, such as statements that the government uses a "Privacy Impact Assessment" process to evaluate privacy in major records systems before they are implemented, have done little or nothing to prevent sensitive information on innocent people from being retained in this massive database.[35] Similarly, repeated assurances that information is "minimized" in accordance with Executive Order 12333 have apparently not prevented at least 560 million records from being warehoused.

Information Sharing Has Been Implemented But Not Fully Assessed. The General Counsel has indicated that the FBI does not set limits on other agencies with access to

---

person who engages as a business or network in the transmission of funds domestically or internationally; (S) a telegraph company; (T) automobile, airplane, and boat sellers; (U) persons involved in real estate closings; (V) the US Postal Service; (W) an agency of the US Government or certain described State or local government agencies; (X) certain casinos; (Y) any business or agency which engages in any activity which the Secretary of the Treasury determines, by regulation, to be an activity which is similar to, related to any business described above; (Z) any other business designated by the Secretary whose cash transactions have a high degree of usefulness in criminal, tax, or regulatory matters or any futures merchant, commodity trader, or commodity pool operator under the Commodity Exchange Act.).

31 NSL Audit at p. 28.

32 *Id.* at p. 30.

33 *Id.* at p. 53.

34 Written Statement of Michael F.A. Morehart, FBI Section Chief, Terrorist Financing Operations Section, Counterterrorism Division, House Committee on Financial Services, May 26, 2005.

35 *See* Written Statement of Maureen A. Baginski, FBI Executive Assistant Director-Intelligence, submitted to Subcommittee on Crime, Terrorism, and Homeland Security of the House Judiciary Committee, April 19, 2005.

these millions of records from conducting data-mining.[36] And nothing appears to limit such sharing to officials engaged in counter-terrorism efforts, and even those number in the tens of thousands. For example, Section 203 of the Patriot Act fully authorized the sharing of information gathered by law enforcement agencies with the CIA, DoD, NSA, immigration, the Secret Service, and White House officials, as long as the use is within their official responsibilities. In short, we have opened the floodgates. We have not yet assessed what has been inundated by this flood of information, such as how increased noise affects effectiveness in preventing attacks or how our privacy has been genuinely harmed—setting aside anecdotal evidence and boilerplate assurances.

Congressional Intervention Is Needed to Protect Privacy and Civil Liberties. At the administration's behest, Congress has allowed the rapid expansion of broad new information gathering powers to sweep in information on innocent bystanders while deferring to the Executive Branch to enact internal rules to protect Americans' privacy. That is a delegation doomed to failure, in my view. All the incentives in execution are to gather more information and share it faster. And the NSL statutes offer little meaningful protection against abuse, given the way NSLs have been handled for the past five years. Congress is more accountable to the people than Executive Branch agencies and should intercede to ensure that privacy and civil liberties are protected. Neither the agencies nor the fundamentally flawed Privacy and Civil Liberties Oversight Board are adequate substitutes for the checks and balances of congressional oversight and investigation.

There Are Privacy Interests in Records Held by Third Parties. Some are not troubled by such privacy concerns because they believe Americans simply have no cognizable privacy interest in any information provided to third parties. I disagree with the claim, for example, that Supreme Court decisions from the 1970s allowing access to certain bank records or phone records without probable cause settled this issue, especially given the technological changes in the past thirty years.[37] And Americans do not believe that just because they bank or use a phone or have health insurance they have waived any privacy interest in their personal information and therefore the government can simply buy it or demand it—unless they have done something wrong. Congress has also taken issue with the narrow approach of the Supreme Court by enacting laws to protect, for example, Americans' financial privacy,[38] the privacy of their credit information,[39] the need for confidentiality in their health matters,[40] and the importance of privacy in educational records.[41] While these privacy statutes provide exceptions for certain investigations, what

---

36 *See* March 20, 2007 HJC transcript at p. 50 (Senator Berman asked "Is it possible that other agencies of the federal government or anywhere are using information in that investigative data warehouse for data mining purposes?" and Ms. Caproni replied, "For data mining purposes -- I don't know the answer to that. I mean, they could get access to it as appropriate for their agency."). Notably, the forthcoming DOJ report on data mining will be produced by the Attorney General's office, and will not be a product of the Inspector General's office.

37 *But see* United States v. Miller, 425 U.S. 435, 443 (1976) (regarding checks); Smith v. Maryland, 442 U.S. 735, 743 (1979) (regarding phone numbers called).

38 Right to Financial Privacy Act (RFPA), Section 1114, Pub. L. No. 95-630, 92 Stat. 3706 (1978).

39 *See, e.g.,* Fair Credit Reporting Act (FCRA) of 1970, as amended, 15 U.S.C. 1681.

40 Health Insurance Portability and Accountability Act (HIPAA) of 1996, 42 U.S.C.§ 1320d et seq.

41 Family Education Rights and Privacy Act of 1974 (FERPA, known as "the Buckley Amendment"), 20 U.S.C. 1232g.

constitutes an investigation has changed dramatically post-Patriot with the modifications to the Attorney General guidelines. And, simply because some such information may be obtained in grand jury investigations under the auspices of officers of the court, that does not mean sensitive records should be available on demand and without check in a preliminary inquiry by FBI agents without any of a reasonable indication of violence.

It Seems Easy to Get Included in the Data Warehouse but You Can't Really Get Out. One of the emerging problems with the widespread use of such secret information gathering tools is that you do not know if your sensitive information is in the Data Warehouse. Even if you discovered your data were in there, it is unclear if or how you get out. And it is unclear how your inclusion might affect your right to travel or work. There appears to be no real way for a person to correct incorrect information which has been widely shared. There do not appear to be sufficient external controls to prevent misuse or abuse or correct mistakes. We do not object, of course, if there is reason to believe a person were planning a terrorist act, but the Patriot Act went too far, too fast. The lack of independent checks on NSLs affects the quality and quantity of data transmitted to the Data Warehouse and, as the IG noted, non-verified information may be disseminated.[42]

The Claims of No Abuses and Adequate Internal Controls Were Unfounded. Let me conclude with a few observations. This Committee and the American people were told repeatedly—before, during and after the Patriot Act reauthorization debate—there had been no abuses of power or civil liberties. The truth is that the administration's approach to problems with NSLs, in spite of repeated questions about checks on these intrusive powers, was that "they didn't look for any and they didn't find them," as the Inspector General agreed was the case before the Senate Judiciary Committee.[43] This variation of "don't ask, don't tell" left Congress and the American people in the dark. As Senator John Sununu, who initially supported the filibuster of the Patriot Act reauthorization bill but then voted for it, recently stated: "They gave us assurances that when we raised concerns about civil liberties that they have strong procedures and checks in place for issuing national security letters, and all of those assurances have proven to be unfounded."[44]

The Administration Sought to Hide the Widespread Use of NSLs. At the same time, it is clear that some in the administration did know that the truth about National Security Letters would undermine their claims that such powers were being used judiciously. I say this for two main reasons.

One, the administration resisted every effort to let the American people know even the ballpark number of NSL requests—perhaps the biggest use of Patriot Act powers--while they selectively de-classified the number of times other powers were used. For example, they chose to reveal there had been about fewer than three dozen FISA court orders for

---

42 NSL Audit at p. 55.

43 *See* Testimony of Inspector General Glenn Fine before the Senate Judiciary Committee on March 21, 2007, available in the CQ SJC Transcript of March 21, 2007 at p. 27. The Inspector General told the Committee that "the FBI was not aware of these problems. They did not have a handle on the scope of the problems." Senator Whitehouse responded, "They didn't look for them and they didn't find them," and Mr. Fine replied, "I think that's correct."

44 Statement of March 14, 2007, available at www.sununu.senate.gov.

records as of April 2005, under Section 215 of the Patriot Act, while hiding the fact there had been at least 1,000 times as many requests under the NSL powers in a single year.[45]

Two, the annual public report added by Patriot reauthorization excluded requests for telephone or e-mail subscriber information,[46] and we question whether Congress was fully informed of the basis for this omission. The administration knew for certain that this was the largest number of NSL requests--one investigation alone swept in over 12,000 subscribers.[47] The public numbers reported in 2006 were skewed to leave a false impression of how focused the powers were. There's a big difference between 9,000 NSL requests per year and 45,000[48]—and it is not just that this is limited to citizens, as the FBI consistently failed to track that pertinent data.[49] And, although this Committee received more information and larger numbers behind closed doors, the IG has said those numbers were "significantly understated."[50] Unfortunately, the Committee was misinformed.

We Appreciate Congress' Determination to Have an Audit to Get the Truth. The audit we are discussing today was ordered by Congress, and we thank you for that. But for this congressionally mandated audit, the administration would have continued to reassure you and the American people that there were adequate safeguards on NSLs to protect civil liberties. This report only underscores the need for Inspector General audits in other critical areas, including other sources of FBI information, such as any contractual arrangements with electronic communications service providers or commercial data brokers, such as Choicepoint, as well as the way data mining is being used. In addition, we believe there should be a comprehensive audit going back to September 11th on the warrantless wiretapping program—including how many conversations and communications have been acquired over this period and what has, and has not, been "minimized."

From the outside, there is reason to suspect in a host of areas that the information and assurances you have been given have been closely shaped, polished or distorted. It is difficult to assess the extent of hair-splitting there has been in any reassurances you have received in these areas—for example, in retrospect every use of the word "generally" in administration discussions of FISA court wiretap orders now appears pregnant with hidden meaning. The damage that has been done to trust in these critically important intelligence issues is especially troubling. From this vantage point, getting assurances from the administration is akin to playing poker with someone who has marked the deck—one just does not know what one is missing, although the party on the other side of the table does. I worry that Congress does not have enough access to career Executive Branch experts who know what is really happening on the ground or a way to verify answers provided.

---

45 *See* NSL Audit at p. xvi.
46 USA PATRIOT Improvement and Reauthorization Act, Pub. L. No. 109-177, § 118 (2006).
47 *See* NSL Audit at pp. xviii and 36.
48 Letter from Assistant Attorney General William E. Moschella, Office of Legislative Affairs at DOJ to the Speaker of the House, April 28, 2006 (giving public information on FISA orders and NSLs.)
49 *See* NSL Audit at pp. xx and 124 (indicating that more than half of the NSL requests from 2005 collected information on U.S. persons, but noting that the FBI does not track whether subscriber information that is provided relates to US person or foreign nationals on analysis of data provided).
50 *See id.* at pp. 32-34 and n.71 (noting that it was "impossible to reconstruct the number of NSL requests during the period of review").

NSLs Were Made More Coercive in 2006. Armed with blanket assurances about internal controls that either were not implemented or did not exist, the flawed NSL powers were made more coercive in 2006 in the Patriot Act reauthorization bill.[51] Compliance can now be compelled, as with a subpoena, and violating the gag can be severely punished, even though the standard for challenging the gag is exceedingly unfair. [52] Of course, giving the businesses that receive NSLs the right to challenge them was the right thing to do, but it is nowhere close to a sufficient check on these intrusive powers. Indeed, it is probably more cost-effective for some businesses to turn over information that they will never have to account for rather than pay lawyers to fight them, and, for some, cooperation may even be a lucrative venture. Congress should reconsider the NSL changes made in 2006.

Internal Controls Are Not Enough—HR 4570 Is a Good Start for Reform. In light of all this, it should be clear that more internal controls within the FBI are not enough to bring the NSL powers under control. History, including this most recent history of the abuse of NSL powers, demonstrates why we must have independent checks and balances.

A good place to start would be to take up the legislation introduced by the former Ranking Member of this Committee, Congresswoman Jane Harman and other Committee Members who are sitting on the dais today, Chairman Reyes, Congressman Hastings, Congressman Boswell, Congressman Cramer, Congresswoman Eshoo, Congressman Holt, Congressman Ruppersberger, and Congressman Tierney, as well as Congressman Berman. We commend you all for the foresight to call for critically important NSL reforms, even before the problems with this power were publicly documented through this audit.

HR 4570, introduced in the 109th Congress, would require there to be a connection between the record sought and a suspected terrorist and would provide an appropriate system for expedited judicial review. It would also require the destruction of sensitive information obtained on people who are cleared or not reasonably suspected of wrongdoing in the course of a proper investigation. Some additional improvements are needed based on new revelations in the audit. For example, Congress needs to address the way the FBI has claimed a power to open "umbrella investigations" with inadequate factual predicates and should add needed checks against the broad approach the FBI has taken to obtain "voluntary" access to sensitive records under the guise of an emergency.

A sunset provision and additional mandated audits on substantive matters related to NSLs and other intrusive powers would also be helpful to protecting both security and privacy. We hope these common sense improvements to safeguard our lives and our liberty will be embraced on a bipartisan basis in light of the stunning revelations in the IG's NSL audit.

Thank you again for considering the views of the Center for National Security Studies.

---

51 *See* USA PATRIOT Improvement and Reauthorization Act, Pub. L. No. 109-177 (2006).
52 It is also important to note that two federal courts found aspects of NSL powers unconstitutional. In one case, DOJ dropped its appeal last year, allowing the librarians who received demands for patron Internet records to speak out but only after the Patriot Act was reauthorized. *See Doe v. Gonzales*, No. 05-0570-cv, (2nd Cir, Apr. 12, 2006). The other NSL challenge, which was also decided on First Amendment grounds, is on remand to the district court based on the 2006 changes. *See Doe v. Ashcroft*, 04 Civ 2614 (VM), (S.D.N.Y) (no final decision yet).