Testimony of

The Honorable Robert S. Mueller, III

Director
Federal Bureau of Investigation
March 27, 2007

Statement of Robert S. Mueller, III Director Federal Bureau of Investigation Before the United States Senate Committee on the Judiciary March 27, 2007

Good morning Mr. Chairman, Senator Specter, and Members of the Committee. Thank you for opportunity to testify before you this morning. Last week, the Committee heard testimony from Glenn Fine, the Inspector General of the Department of Justice regarding a recent report issued by his office on the FBI's use of national security letters, or NSLs. The Inspector General and his staff conducted a thorough and fair review of this authority and the Congress is to be commended for requiring that this review be conducted. As you heard from the Inspector General, he did not find any deliberate or intentional misuse of the national security letter authorities, Attorney General Guidelines or FBI policy. Nevertheless, the review by the Office of Inspector General (OIG) identified several areas of inadequate auditing and oversight of these vital investigative tools, as well as processes that were inappropriate. Although not intentionally, we fell short in our obligations to report to Congress on the frequency with which we use this tool and in the internal controls we put into place to make sure that it was used only in accordance with the letter of the law. I take responsibility for those shortcomings and for taking the steps to ensure that they do not happen again. The OIG report made ten recommendations designed to provide both the necessary controls over the issuance of NSLs and the creation and maintenance of accurate records. I fully support each recommendation and concur with the Inspector General that, when implemented, these reforms will ensure full compliance with both the letter and the spirit of the authorities entrusted to the Bureau by the Congress and the American people.

National Security Letters generally permit us to obtain the same sort of documents from third party businesses that prosecutors and agents obtain in criminal investigations with grand jury subpoenas. Unlike grand jury subpoenas, however, NSL authority comes through several distinct statutes and they have specific rules that accompany them. NSLs have been instrumental in breaking up cells like the "Portland Seven," the "Lackawanna Six," and the "Northern Virginia Jihad." Through the use of NSLs, the FBI has traced sources of terrorist funding, established telephone and e-mail linkages that resulted in further investigation and arrests, and arrested suspicious associates with deadly weapons and explosives.

National Security Letter Authorities

The NSL authority used most frequently by the FBI is that provided by the Electronic Communications Privacy Act (ECPA). Through an ECPA NSL, the FBI can obtain subscriber information for telephones and electronic communications and can obtain toll billing information

and electronic communication transaction records. Significantly, the FBI cannot obtain the content of communications through an ECPA NSL. Although the exact numbers of ECPA NSLs remains classified, it is the most common NSL authority used.

Pursuant to the Right to Financial Privacy Act (RFP A), the FBI also has the authority to issue NSLs for financial records from a financial institution. RFPA NSLs are used commonly in connection with investigations of potential terror financing.

Pursuant to the Fair Credit Reporting Act, the FBI has the authority to issue three different, but related, types ofNSLs to credit reporting agencies: an NSL pursuant to 15 V.S.C. 1681u(a) for the names of fmancial institutions with which the subject has or has had an account; an NSL pursuant to 15 V.S.C. l68lu(b) for consumer identifying information (name, address, former addresses, employment and former employment); an NSL pursuant to 15 U.S.C. l68lv for a full credit report. Of all the FBI"s NSL authorities, only the last of the FCRA authorities is restricted to use only in international terrorism cases.

Finally, the FBI has the authority to issue NSLs pursuant to the National Security Act in the course of investigations of improper disclosure of classified information by government employees.

For the first 3 types ofNSLs (ECPA, RFPA, FCRA) the NSL must include a certification by an authorized FBI employee that the material is being sought for an authorized national security investigation. That certification is slightly different in the case of a FCRA NSL for a full credit report, where the certification required is that the information is relevant to an international terrorism investigation.

The authority to issue an NSL lies at a senior level within the FBI. An NSL can be issued only by an official who ranks not lower than Special Agent in Charge or Deputy Assistant Director. All such officials are career government employees who are members of the Senior Executive Service. Procedurally, an agent or analyst 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 investigation. Additionally, it needs to provide sufficient information concerning the underlying investigation so that reviewing officials can confirm that the investigation is adequately predicated and not based solely on the exercise of First Amendment rights. Finally, the EC includes a "lead" to the Office of the General Counsel (OGC) for purposes of Congressional reporting.

The OIG Report

As directed by Congress, we endeavored to declassify as much information as possible concerning our use of NSLs in order to allow the maximum amount of public awareness of the extent of our use of the NSL tool consistent with national security concerns. To that end, for the first time the public has a sense of the frequency with which the FBI makes requests for data with national security letters. In the period covered by the report, the number of NSL requests has ranged from approximately 40,000 to 60,000 per year and we have requested information on less than 20,000 persons per year. For a variety of reasons that will be discussed below, those

numbers are not exact. Nevertheless, they, for the first time, allow the public to get some sense of the order of magnitude of these requests; there are a substantial number of requests, but we are not collecting information on hundreds of thousands of Americans.

There are three findings by the OIG that are particularly disturbing, and it is those three findings that I wish to address this morning: (l) inaccurate reporting to Congress of various data points we are obligated to report relative to NSLs; (2) the use of so-called exigent letters that circumvented the procedures required by ECPA; and (3) known violations (both previously self reported by FBI and not previously reported) of law and policy with regard to usage of NSLs.

Congressional Reporting

A finding of the report that particularly distresses me is the section that addresses the inaccuracies of the numbers we report to Congress. The process for tabulating NSLs simply did not keep up with the volume. Although we came to that realization prior to the OIG report and are working on a technological solution, that realization came later than it should have.

The tracking of NSLs for Congressional reporting purposes resides in a standalone Access database. This database is referred to in the OIG report as the OGC database. While the OGC database was a major technological step forward from 3 x 5 index cards once used to track NSLs, it is not an acceptable system given the significant increase in use of NSLs since 9/11. First and foremost, the OGC database is not electronically connected to ACS, the system from which we derive the data. Instead, there is a manual interface between ACS and the OGC database. An OGC employee is responsible for taking every NSL lead that is sent to OGC and manually entering the pertinent information into the aGC database. Nearly a dozen fields must be manually entered, including the file number of the case in which the NSL was issued (typically 15 digits and alphanumeric identifiers).

Approximately a year ago, we recognized that our technology was inadequate and began developing an automated system to improve our ability to collect this data. The system, in addition to improving data collection, will automatically prevent many of the errors in NSLs that we will discuss today. We are building an NSL system to function as a workflow tool that will automate much of the work that is associated with preparing NSLs and the associated paperwork. The NSL system 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 automatically ensure that certain legal and administrative requirements are met and that required reporting data is accurately collected. For example, by requiring the user to identify the investigative file from which the NSL is to be issued, the system will be able to verify the status of that file to ensure that it is still open and current (e.g. request date is within six months of the opening or an extension has been filed for the investigation) and ensure that NSLs are not being requested out of control or administrative files. The system will require the user to separately identify the target of the investigative file and the person whose records are being obtained through the requested NSL, if different. This will allow the FBI to accurately count the number of different persons about whom we gather data through NSLs. The system will also require that specific data elements be entered before the process can continue, such as requiring that the target's status as a United States Person or non-United States Person be

entered. The system will not permit requests containing logically inconsistent answers to proceed.

The NSL system is being designed so that the FBI employee requesting an NSL will enter data only once. For example, an agent or analyst who wishes to get telephone toll billing records will only have to prompt the system that he is seeking an ECPA NSL for toll records and type the telephone number once. The system will then automatically populate the appropriate fields in the NSL and the authorizing EC. The system will then generate both the NSL and the authorizing EC for signature, thereby ensuring that the two documents match exactly and minimizing the opportunity for transcription errors that give rise to unauthorized collections that must be reported to the Intelligence Oversight Board (lOB). Agents and analysts will still be required to provide the narrative necessary to explain why the NSL is being sought, the factual basis for making a determination that the information is relevant to an appropriately predicated national security investigation, and the factual basis for a determination whether the NSL should include a non-disclosure provision. In addition, this system will have a comprehensive reporting capability.

We began working with developers on the NSL system in February 2006 and we are optimistic that we will be able to pilot it this summer and roll it out to all field offices by the end of the year. At that point, I will be confident the data we provide to Congress in future reports is as accurate as humanly possible.

In the meantime, we are taking several steps to correct the numbers we have previously reported. First, we are making data corrections in our database. Through a computer program, we have identified all entries that must be erroneous because there is an apparent error in the entry (e.g., there are more NSLs reported than requests; the date shows a year that is impossible (203)). We are manually reviewing those entries and making corrections. We have also started a random sampling often percent of the total entries in the OGC database which contains approximately 64,000 entries. Those entries will be manually checked against ACS. We will determine whether there is a significant difference between the entries in our database and the actual information in ACS. To the extent there is a difference, that will be the factor that will be used to correct our prior reporting. While not yielding an exact count, we believe that to be a statistically appropriate way of correcting prior reporting. We have discussed this methodology with the OIG and will offer it the opportunity to review our work. We are striving to have corrected reports to Congress as soon as possible.

As with the other shortcomings identified by the OIG, there was no finding of an intent to deceive Congress concerning our use of NSLs. In fact, as noted, we identified deficiencies in our system for generating data prior to the initiation of the OIG's review and flagged the issue for Congress almost one year ago. While we do not know the extent of the inaccuracies in past reporting, we are confident that the numbers will not change by an order of magnitude.

Exigent Letters

The next significant finding of the OIG involved the use within one unit at Headquarters of so-called "exigent letters." These letters, which numbered in excess of 700, were provided to telephone companies with requests for toll billing information regarding telephone numbers. All of the letters stated that there were exigent circumstances. Many of the letters stated that federal

grand jury subpoenas had been requested for the records even though in fact no such request for grand jury subpoenas had been made, while others promised future national security letters. From an audit and internal control perspective, the FBI did not document the nature of the emergency circumstances that led it to ask for toll records in advance of proper legal process, did not keep copies of all of the exigent letters it provided to the telephone companies, and did not keep records showing that it had subsequently provided either the legal process promised or any other legal process. Further, based on interviews the OIG conducted, some employees indicated that there was not always any emergency relating to the documents that were sought.

OGC has been working with the affected unit to attempt to reconcile the documentation and to ensure that any telephone record we have in an FBI database was obtained because it was relevant to an authorized investigation and that appropriate legal process has now been provided. As of late last week, there were still a small handful of telephone numbers that had not been satisfactorily tied to an authorized investigation. If we are unable to determine the investigation to which those telephone numbers relate, they will be removed from our database and destroyed.

The OIG rightfully objected to the FBI obtaining telephone records by providing a telephone carrier with a letter that states that a federal grand jury subpoena had been requested when that was untrue. It is unclear at this point why that happened. I have ordered a special inspection in order to better understand the full scope of internal control lapses. We also concur with the OIG that it is inappropriate to obtain records on the basis of a purported emergency if, in fact, there is no emergency. We continue to believe, however, that providers had the right to rely on our representation that there was an emergency and that the "exigent letters" - had they been issued only when there was an exigent circumstance and had they correctly identified the legal process that would follow - would have been an appropriate tool to use.

In response to the obvious internal control lapses this situation highlights, changes have already been made to ensure that this situation does not recur. Any agent who needs to obtain ECPA-protected records on an emergency basis must now do so pursuant to 18 v.s.e. 2702. Section 2702(c)(4) permits a carrier to provide information regarding its customers to the government if the provider in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to . the emergency. A request for disclosure pursuant to that statute generally must be in writing and must clearly state that the disclosure without legal process is at the provider's option. The letter request must also set out the basic facts of the emergency so that the provider can make some assessment whether it concurs that there is an emergency.

Intelligence Oversight Board Process

The OIG also examined misuse of NSLs that had been reported (and some that had not been reported) as part of the IOB process. As this committee knows, pursuant to Executive Order 12863 the President has an Intelligence Oversight Board that receives from the agencies in the intelligence community reports of intelligence activities that the agency believes may have been unlawful or contrary to Executive Order or Presidential Directive. This language is interpreted by the FBI and DOJ to mandate the reporting of any violation of a provision of the Attorney

General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection if such provision is designed to ensure the protection of individual rights.

The FBI requires its employees to report any violations of law or policy about which they are aware. We encourage employees to err on the side of reporting so that we can be sure that all violations are appropriately reported. In terms of process, all potential violations are reported to OGC. Lawyers within OGC are responsible for adjudicating" the violation that is, determining whether the potential violation is an actual Intelligence Oversight Board violation. If it is, a report is made to the IOB, a copy is provided to DOJ and a copy is provided to the FBI's Inspection Division. If the violation involved intentional misconduct, the Inspection Division will determine whether the matter should be referred to the Office of Professional Responsibility for discipline.

The OIG found that from 2003 through 2005, the FBI had self-reported 26 potential violations involving NSL authorities. Of the 26, OGC adjudicated 19 to be violations and reported them. The OIG agreed with each of those determinations. Of the 7 potential violations that OGC determined were not violations, the OIG agreed with all but one. As to the one determination about which we disagreed, upon re-review, the FBI concurred with the OIG that it was a violation that should have been reported and it has since been reported to the lOB. These 20 violations included: third party errors (4), NSLs issued when the authority for the investigation had lapsed (3), obtaining ECPA-protected records without any legal process (3) and obtaining a full credit report in a counterintelligence case (1).

The OIG also found, however, a number of potential IOBs in the files it examined that had not been reported to OGC for adjudication. The OIG examined 293 NSLs - a reasonably small sample. The sample was a judgmental sample and the size was chosen because the audit was extremely labor intensive. We do not suggest that the sample was not a fair sample (although it was not random), but only that it is questionable from a statistical standpoint to attempt to extrapolate from a very small sample to an entire population. Moreover, there was wide variation in the number of purported unreported violations from different field offices. The OIG found 8 potential violations that were unreported in files in both the Philadelphia and Chicago field offices, but only 2 unreported potential violations from files in New York and 4 from San Francisco. We are doing additional follow-up work, but the wide variance between field offices may be a function of the very small sample, or it may indicate that the percentages of potential errors detected are not constant across all field offices.

Of the 293 NSLs the OIG examined, 22 (7%) were judged to have potential unreported IOB violations associated with them. Moreover, of those 22 NSLs, 10 - or almost 50% - were third party errors -- that is, the NSL recipient provided the FBI with information we did not seek. Only 12 of the NSLs examined - 4% - had mistakes that the OIG rightfully attributes to the FBI.

Examining the 12 potential errors that were rightfully attributed to the FBI reveals a continuum of seriousness relative to the potential" impact on individual rights. Four (or just over 1% of the sample) were serious violations. Specifically, two of the violations involved obtaining full credit reports in counterintelligence investigations (which is not statutorily authorized), one involved issuing an NSL when authorization for the investigation to which it related had lapsed, and one involved issuing an NSL for information that was arguably content, and therefore not available

pursuant to an NSL. (In the latter case, the ISP on which the NSL was served declined to produce the requested material so there was, in fact, no collection of information to which we were not entitled.) The balance of the 12 potential violations identified by the OIG do not, in our view, rise to the same level of seriousness as those 4. The remaining 8 involve errors that are best characterized as arising from a lack of attention to detail, and did not result in the FBI seeking or obtaining any information to which it was not entitled. Those 8 potential violations involved errors such as using the wrong certification language in an NSL (although the appropriate certification is not materially different) and having the NSL and the EC seeking the NSL not entirely consistent. We do not excuse such lack of attention to detail, but we do not believe that such mistakes result in or cause a risk to civil liberties.

In short, approximately 1% of the NSLs examined by the OIG had significant errors that were attributable to FBI actions and that had not been, but should have been, reported as potential lOB violations.

While a 1% error rate is not huge, it is unacceptable, and we have taken steps to reduce that error rate. First, we are very concerned that of all the potential IOBs involving mistakes in NSLs attributable to the FBI (whether previously reported or not), 3 involved the same mistake: namely, issuing an NSL for a full credit report in a counterintelligence investigation. In order to ensure that this particular error is fully rectified, I have ordered all FBI field offices to examine all counterintelligence files in which Fair Credit Report NSLs have been issued since January 1, 2002 in order to ascertain whether the file contains a full credit report. If it does, the credit report must be removed from the file, sequestered with the field office's attorney, and a potential IOB violation must be reported to OGC. The results from that search are due to headquarters by mid-April 2007.

Additional Corrective Steps

Several other steps we have taken will, we believe, reduce the likelihood that the FBI will commit the other mistakes in the future. First, as indicated previously, the FBI is developing an automated system to prepare NSLs and their authorizing ECs. That system will reduce to zero mistakes such as having the wrong certification language or inconsistency between the NSL and the EC. It will also ensure that the investigative file out of which the NSL is being issued is open. Finally, it will ensure that an NSL for a full credit report cannot be issued out of a counterintelligence file.

Other changes to FBI policy have been made that we believe will facilitate better handling of IOBs and also reduce errors that lead to IOBs. First, last fall we provided comprehensive advice to the field regarding its responsibility towards information obtained as a result of third party errors. That guidance requires all such information to be sequestered and reported to OGC as a potential IOB. If the "over collected" information is irrelevant to the investigation (e.g., the telephone company transposed a number and provided us records on the wrong telephone account), then it will be destroyed or returned. No such information should be entered into FBI databases. If the information is relevant to the investigation but simply not within the four comers of the NSL, then the information must be sequestered until a new NSL has been issued for the extra data. After the new NSL has been issued, the information can be entered into FBI databases.

Secondly, we have collected all the rules and policies on NSLs into one document which will be disseminated to the field. Those rules now mandate that, until the deployment of the automated NSL system, all NSLs and ECs be prepared from the exemplars that are provided on OGC's website. That should eliminate many of the mistakes identified by the OIG.

All of these rules will, of course, only reduce or eliminate errors if they are followed. The OIG's report has highlighted for us that there must be some sort of auditing function - above and beyond the IOB process - to systematically ensure that these rules, as well as others that govern our activities in national security investigations are followed. The FBI has historically been very good at establishing policy and setting rules, but we have not been as proactive as we should have been in establishing internal controls and auditing functions.

The full parameters of the compliance program have not been set, although these aspects have been: the Inspection Division with participation of DOJ's National Security Division and Privacy and Civil Liberties Office is in the process of a special inspection of NSL usage in all 56 field offices and headquarters. That inspection should uncover any other significant problems with our use of this tool but should also tell us whether there are variances between offices in terms of the numbers and types of errors. The results of the inspection will then inform the program that the Attorney General announced of having teams of DOJ lawyers, FBI lawyers and the Inspection Division periodically audit field offices' use of NSLs. That process will begin in April and should result in at least 15 offices being audited this year. We are also considering other proactive compliance programs in order to develop a program that ensures, to the maximum extent possible, that the rules and policies designed to protect privacy and civil liberties are faithfully adhered to by all of our employees, that we promptly identify and correct any violations of law or policy, and that any information collected erroneously is removed from FBI databases and destroyed. In addition, a working group co-chaired by the Office of the Director of National Intelligence and the CPCLO has been convened to examine how NSL derived information is used and retained by the FBI. The FBI and DOJ's National Security Division will have a representative on this working group. We welcome the Committee's input as we move forward on these initiatives.

Mr. Chairman, the FBI is acutely aware that we cannot protect against threats at the expense of civil liberties. We are judged not just by our ability to defend the nation from terrorist attacks but also our commitment to defend the rights and freedoms we all enjoy. In light of the Inspector General's findings, we are committed to demonstrating to this Committee, to the Congress, and to the American people that we will correct these deficiencies and utilize the critical tools Congress has provided us consistent with the privacy protections and civil liberties that we are sworn to uphold.

I appreciate the opportunity to appear before the Committee and look forward to answering your questions. Thank you.