Statement of
Valerie E. Caproni
General Counsel
Federal Bureau of Investigation
Before the
Committee on the Judiciary
United States House of Representatives
Subcommittee on the Constitution, Civil Rights, and Civil Liberties
Concerning
National Security Letters
April 15, 2008

Good afternoon Mr. Chairman, Ranking Member Franks, and Members of the Subcommittee. It is my pleasure to appear before you today to discuss with the Subcommittee the FBI's use of national security letters (NSLs), particularly in light of the Inspector General's report released on March 9, 2007, and his follow-on report released on March 13, 2008. The IG's reports are fair, acknowledging the importance of NSLs to the ability of the FBI to conduct the national security investigations that are essential to keeping the country safe. Importantly, the Office of the Inspector General (OIG) found no deliberate or intentional misuse of the NSL authorities, Attorney General Guidelines, nor FBI policy. Furthermore, I want to emphasize two extremely important points regarding the IG's second report (i.e., the one released on March 13, 2008). That report covered 2006, before the FBI had in place its modifications designed to ensure the NSL problems the IG identified in his initial report are not repeated. As a result, the problems addressed in the second report obviously do not reflect a failure to respond to the 2007 IG report. Second, we appreciate that the IG in his second report found that we have made

tremendous strides in resolving the problems previously identified and that we appear to be on track to implementing policies and procedures to minimize the likelihood that the problems will recur. Specifically, the IG found that the FBI has made significant progress responding to the issues raised in the first report and that the FBI's leadership has made this issue a top priority.

Although not intentionally, we fell short in our obligation to report to Congress on the frequency with which we use this tool and in establishing rigorous internal controls to ensure all NSLs were served strictly in accordance with legal requirements and to ensure that any materials received from third parties were in strict compliance with the NSL served on that party. Director Mueller concluded from the IG's 2007 report that we need to redouble our efforts to ensure that there would be no repetition of the mistakes of the past, however lacking in willfulness, and I share his commitment. We appreciate the attention of Congress to these audits, which were called for in the USA PATRIOT Improvement and Reauthorization Act. We welcomed the OIG's reviews regarding this important tool's use. The first report made 10 recommendations and the second made 17 recommendations. The recommendations were designed to provide controls over the issuance of NSLs, the creation and maintenance of accurate records necessary for Congressional reporting and procedures to ensure that "over productions" (i.e., records from NSL recipients that were not called for by the NSL) were appropriately handled. The FBI fully supports each of the 27 recommendations and concurs with the IG that, when implemented, these reforms will ensure full compliance with both the letter and the spirit of the authorities entrusted to the Bureau.

H.R. 3189

We are aware of H.R. 3189, currently titled as the proposed National Security Letters Reform Act of 2007, that was introduced last July and subsequently referred to this Subcommittee last September. Important to the consideration of any legislative changes are the many oversight and internal control mechanisms that the FBI has established since the release of

the IG's first report. We believe these are important steps and that, in light of the FBI's tremendous progress in this regard, further legislative changes, including the measures envisioned by H.R. 3189, would be neither necessary nor appropriate.

FBI Corrective Measures

Several years ago, the FBI's process for tracking NSLs for Congressional reporting purposes shifted from a totally manual process, where NSL data were written on 3 x 5 cards, to a standalone Access database. This database is referenced in the first IG report as the OGC database. While the OGC database was a giant technological step forward from 3 x 5 cards, it was not an adequate system given the increase in NSL usage since 9/11. Approximately two years ago, we recognized that our technology was inadequate, and we began developing a system for improved data collection. The new system, in addition to improving data collection, now automatically prevents many of the NSL-related errors referenced in the IG reports. Specifically, we built an NSL subsystem within the already existing, highly successful FISA Management System (FISAMS) to function as a workflow tool that automates much of the work in preparing NSLs and their associated paperwork. The NSL subsystem 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 verifies the status of that file to ensure that it is still open and current, and it ensures that NSLs are not being requested out of control or administrative files. The system requires the user to identify separately the target of the investigative file and the person about whom records are being obtained through the requested NSL, if different. This allows the FBI to count accurately the number of different persons about whom we gather data through NSLs. 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 U.S. Person (USPER) or non-USPER be entered. 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 enters data only once. Among other things, this minimizes transcription errors that give rise to unauthorized collections that must be reported to the Intelligence Oversight Board (IOB). In addition, requesters are 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 basis for a determination that the NSL should include a non-disclosure provision, if such a provision is included within that particular NSL. As with the FISA Management System, this subsystem has a comprehensive reporting capability.

We began working with developers on the NSL subsystem in February 2006, and after a brief piloting period, its rollout was completed on January 1, 2008. Now, as we move forward, and as we continue to make minor system modifications to address certain situations, I am more confident that the data we report to Congress on NSLs issued subsequent to January 1, 2008 will be as accurate as possible.

One particularly significant finding in the IG's first report involved the use within one unit at Headquarters of so-called "exigent letters." These letters 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 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 the exigent letters it provided to the telephone companies, and did not keep records showing whether it had subsequently provided either the legal process promised or any other legal process. Further, based on interviews the IG conducted, some employees indicated that there was not always any emergency relating to the documents that were sought.

The FBI is working jointly with the IG in its investigation of the exigent letter situation. Because that matter is still under investigation, I cannot address it in any depth. However, I would like to emphasize that, in response to the obvious internal-control lapses this situation highlights, changes have already been made to ensure that this situation does not recur. Now, any agent who needs to obtain records protected under the Electronic Communications Privacy Act (ECPA) on an emergency basis must do so pursuant to 18 U.S.C. § 2702. Section 2702(c)(4) permits a carrier to provide non-content 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[.]" Although not required by the statute, FBI policy requires that a request for such disclosure generally must be in writing and must clearly state that the disclosure without legal process is at the provider's option. The request for documents must be approved at a level not lower than Assistant Special Agent in Charge (ASAC) in a field office and not lower than Section Chief at Headquarters. The letter request must set out the basic facts of the emergency so that the provider can make some assessment whether it concurs that there is an emergency. In addition, the fact that documents were obtained pursuant to a 2702 letter as well as ASAC approval must be documented in an Electronic Communication (EC). While the policy allows for oral approval by the ASAC, OGC requires that the approval be documented after the fact if it is not possible to do so prior to receipt of the records. We believe this policy permits our agents to obtain quickly telephone records in cases of true emergency while creating strong internal control mechanisms, which are subject to audit, to ensure that 2702 is not abused.

One important realization--across the board, not merely in the context of NSLs--was that, although the FBI generally had appropriate procedures in place, it did not have an effective mechanism to ensure that the procedures were being followed. As a result, the Director established a new Office of Integrity and Compliance, reporting to the Deputy Director, to identify proactively those areas where there are weaknesses or potential weaknesses in internal controls, inadequate policies or training, or inadequate compliance mechanisms and to address them. As the Director recently testified before another House Subcommittee: "The lesson we learned from this episode is that it's insufficient to issue procedures without also having a mechanism to assure that the procedures are being followed in our 56 field offices and in our 400 resident agencies."

Other corrective measures the FBI has implemented include, for example, a very important and comprehensive EC, dated June 1, 2007, that set forth in one document all FBI policy regarding NSLs. The preparation of that EC involved, among other things, meetings with various national-level privacy groups and certain congressional staff members. Extremely valuable suggestions resulted from those meetings, many of which were incorporated into the FBI's guidance. The EC and other FBI guidance now require, for example, that all NSLs must be reviewed and approved by a Chief Division Counsel, an Associate Division Counsel, or an attorney within the FBI's National Security Law Branch. These attorneys must provide independent legal review of all NSLs. The guidance also bars the use of exigent letters, requires reviewers to ensure relevance to an open national security investigation and compliance with other statutory and procedural requirements, outlines how so-called “over-collected material” must be handled, and requires signed copies of the NSLs to be retained. Furthermore, to implement these policy changes and to educate FBI employees on common NSL-related problems, we have placed heavy emphasis on NSLs in our training of agents, analysts, and other employees involved in national security investigations. Now, whenever an attorney from the

National Security Law Branch visits a field office, that attorney conducts training on NSLs. In addition, we created a detailed online NSL training course which is required for every employee who is involved in drafting, reviewing, or approving NSLs.

Conclusion

We in the FBI know that we can accomplish our mission of keeping the country safe only if we are trusted by all segments of the American public. With events like the London terror attacks of 3 years ago and the Canadian plot to use fertilizer bombs to destroy buildings in Canada in 2006, we have all been reminded of the risk of a catastrophic attack from homegrown terrorists. Our single best defense against such an attack is the eyes and ears of all Americans--but particularly of those segments of the population in which the risk of radicalization is the highest. We need people in those communities to call us when they hear or see something that looks amiss. We know that we reduce the probability of that call immeasurably if we lose the confidence of those segments of the population. It is for that reason that we continually look for ways to assure all Americans that we respect their individual rights, including privacy rights, and that we use the tools that have been provided to us consistent with the rules set by Congress.

I appreciate the opportunity to appear before the Subcommittee, and look forward to your questions. Thank you.