



**Congressional  
Research Service**

Informing the legislative debate since 1914

---

# National Security Letters in Foreign Intelligence Investigations: A Glimpse at the Legal Background

**Charles Doyle**

Senior Specialist in American Public Law

January 3, 2014

**Congressional Research Service**

7-5700

[www.crs.gov](http://www.crs.gov)

RS22406

## Summary

Five federal statutes authorize intelligence officials to request certain business record information in connection with national security investigations. The authority to issue these national security letters (NSLs) is comparable to the authority to issue administrative subpoenas. The USA PATRIOT Act (107-56) expanded the authority under four of the NSL statutes and created the fifth. Thereafter, the authority has been reported to have been widely used. Prospects of its continued use dimmed, however, after two lower federal courts held that the lack of judicial review and the absolute confidentiality requirements in one of the statutes rendered it constitutionally suspect.

A report by the Department of Justice's Inspector General (IG) found that in its pre-amendment use of expanded USA PATRIOT Act authority the FBI had "used NSLs in violation of applicable NSL statutes, Attorney General Guidelines, and internal FBI policies," but that no criminal laws had been broken. A year later, a second IG report confirmed the findings of the first, and noted the corrective measures taken in response. A third IG report, critical of the FBI's use of exigent letters and informal NSL alternatives, noted that the practice had been stopped and related problems addressed.

The USA PATRIOT Improvement and Reauthorization Act (P.L. 109-177, and its companion, P.L. 109-178) amended the five NSL sections to expressly provide for judicial review of both the NSLs and the confidentiality requirements that attend them. The sections have also been made explicitly judicially enforceable and sanctions recognized for failure to comply with an NSL request or to breach NSL confidentiality requirements with the intent to obstruct justice. The use of the authority has been made subject to greater congressional oversight. Following amendment, a federal district court found the amended procedure contrary to the demands of the First Amendment. The U.S. Court of Appeals for the Second Circuit, however, ruled that the amended statutes could withstand constitutional scrutiny if the government confined itself to a procedure which requires (1) notice to the recipient of its option to object to a secrecy requirement; (2) upon recipient objection, prompt judicial review at the government's petition and burden; and (3) meaningful judicial review without conclusive weight afforded a government certification of risk. Using this procedure, the district court upheld continuation of the *Doe* nondisclosure requirement following an ex parte, in camera hearing and granted the plaintiff's motion for an unclassified, redacted summary of the government declaration on which the court's decision was based. More recently, a district court in the Ninth Circuit agreed the amended nondisclosure and judicial review provisions were constitutionally defective, but could not agree to the Second Circuit's narrowing construction or that the NSL statute could be saved by severing the deficient disclosure provisions. The district court stayed its order enjoining issuance of further NSLs or enforcement of any accompanying nondisclosure provisions, however, pending appeal to the Ninth Circuit.

The President's Review Group on Intelligence and Communications Technologies recommended several NSL statutory adjustments designed to eliminate differences between NSLs and Section 215 orders (under P.L. 107-56), including requiring pre-issuance judicial approval of NSLs.

This is an abridged version of CRS Report RL33320, *National Security Letters in Foreign Intelligence Investigations: Legal Background*, without the footnotes, appendixes, and most of the citations to authority found in the longer report.

## **Contents**

Background.....	1
NSL Amendments in the 109 <sup>th</sup> Congress .....	3
Inspector General’s Reports.....	3
NSLs in Court.....	4
Recommendations of the President’s Review Group.....	5
Comparison of NSL Attributes .....	6

## **Tables**

Table 1. Profile of the Current NSL Statutes .....	7
--	---

## **Contacts**

Author Contact Information.....	8
---------------------------------	---

## Background

The ancestor of the first NSL letter provision is an exception to privacy protections afforded by the Right to Financial Privacy Act (RFPA). Its history is not particularly instructive and consists primarily of a determination that the exception in its original form should not be too broadly construed. But the exception was just that, an exception. It was neither an affirmative grant of authority to request information nor a command to financial institutions to provide information when asked. It removed the restrictions on the release of customer information imposed on financial institutions by the RFPA, but it left them free to decline to comply when asked to do so.

[I]n certain significant instances, financial institutions [had] declined to grant the FBI access to financial records in response to requests under Section 1114(a). The FBI informed the Committee that the problem occurs particularly in States which have State constitutional privacy protection provisions or State banking privacy laws. In those States, financial institutions decline to grant the FBI access because State law prohibits them from granting such access and the RFPA, since it permits but does not mandate such access, does not override State law. In such a situation, the concerned financial institutions which might otherwise desire to grant the FBI access to a customer's record will not do so, because State law does not allow such cooperation, and cooperation might expose them to liability to the customer whose records the FBI sought access. (H.Rept. 99-690, at 15-6 [1986].)

Congress responded with passage of the first NSL statute as an amendment to the RFPA, affirmatively giving the FBI access to financial institution records in certain foreign intelligence cases. At the same time, in the Electronic Communications Privacy Act, it afforded the FBI comparable access to telephone company and other communications service provider customer information. Together, the two NSL provisions afforded the FBI access to communications and financial business records under limited circumstances—customer and customer transaction information held by telephone carriers and banks pertaining to a foreign power or its agents relevant to a foreign counterintelligence investigation. Both the communications provider section and the RFPA section contained nondisclosure provisions and limitations on further dissemination, except pursuant to guidelines promulgated by the Attorney General. Neither had an express enforcement mechanism nor identified penalties for failure to comply with either the NSL or the nondisclosure instruction.

In the mid-1990s, Congress added two more NSL provisions—one permits NSL use in connection with the investigation of government employee leaks of classified information under the National Security Act; the other grants the FBI access to credit agency records pursuant to the Fair Credit Reporting Act, under much the same conditions as apply to the records of financial institutions. The FBI asked for the Fair Credit Reporting Act amendment as a threshold mechanism to enable it to make more effective use of its bank record access authority:

FBI's right of access under the Right of Financial Privacy Act cannot be effectively used, however, until the FBI discovers which financial institutions are being utilized by the subject of a counterintelligence investigation. Consumer reports maintained by credit bureaus are a ready source of such information, but, although such report[s] are readily available to the private sector, they are not available to FBI counterintelligence investigators....

FBI has made a specific showing ... that the effort to identify financial institutions in order to make use of FBI authority under the Right to Financial Privacy Act can not only be time-consuming and resource-intensive, but can also require the use of investigative techniques—such as physical and electronic surveillance, review of mail covers, and canvassing of all

banks in an area—that would appear to be more intrusive than the review of credit reports. (H.Rept. 104-427, at 36 [1996].)

The National Security Act NSL provision authorizes access to credit and financial institution records of federal employees with security clearances who were required to give their consent as a condition for clearance. Passed in the wake of the Ames espionage case, it is limited to investigations of classified information leaks.

Both the Fair Credit Reporting Act section and the National Security Act section contain dissemination restrictions, as well as safe harbor (immunity) and nondisclosure provisions. Neither has an explicit penalty for improper disclosure of the request, but the Fair Credit Reporting Act section expressly authorizes judicial enforcement.

The USA PATRIOT Act amended three of the four existing NSL statutes and added a fifth. In each of the three NSL statutes available exclusively to the FBI—the Electronic Communications Privacy Act section, the Right to Financial Privacy Act section, and the Fair Credit Reporting Act section (§505 of the USA PATRIOT Act)

- expanded FBI issuing authority beyond FBI headquarter officials to include the heads of the FBI field offices (i.e., Special Agents in Charge [SACs]);
- eliminated the requirement that the record information sought pertain to a foreign power or the agent of a foreign power;
- required instead that the NSL request be relevant to an investigation to protect against international terrorism or foreign spying; and
- added the caveat that no such investigation of an American can be predicated exclusively on First Amendment-protected activities.

The amendments allowed NSL authority to be employed more quickly (without the delays associated with prior approval from FBI headquarters) and more widely (without requiring that the information pertain to a foreign power or its agents).

Subsection 358(g) of the USA PATRIOT Act amended the Fair Credit Reporting Act to add a fifth and final NSL section, and the provision had one particularly noteworthy feature: it was available not merely to the FBI but to any government agency investigating or analyzing international terrorism:

Notwithstanding section 1681b of this title or any other provision of this subchapter, a consumer reporting agency shall furnish a consumer report of a consumer and all other information in a consumer's file to a government agency authorized to conduct investigations of, or intelligence or counterintelligence activities or analysis related to, international terrorism when presented with a written certification by such government agency that such information is necessary for the agency's conduct or such investigation, activity or analysis.

Although the subsection's legislative history treats it as a matter of first impression, Congress's obvious intent was to provide other agencies with the national security letter authority comparable to that enjoyed by the FBI under the Fair Credit Reporting Act. The new section had a nondisclosure and a safe harbor subsection, but no express means of judicial enforcement or penalties for improper disclosure of a request under the section.

## NSL Amendments in the 109<sup>th</sup> Congress

Both USA PATRIOT Act reauthorization statutes—P.L. 109-177 (H.R. 3199) and P.L. 109-178 (S. 2271)—amended the NSL statutes. They provided for judicial enforcement of the letter requests and for judicial review of both the requests and accompanying nondisclosure requirements. They established specific penalties for failure to comply or to observe the nondisclosure requirements. They made it clear that the nondisclosure requirements do not preclude a recipient from consulting an attorney. They provided a mechanism to lift the nondisclosure requirement. Finally, they expanded congressional oversight and called for an Inspector General’s audit of use of the authority.

## Inspector General’s Reports

The Department of Justice Inspector General reports, one released in March of 2007, the second in March of 2008, and the third in January of 2010, were less than totally favorable. The first report noted that FBI use of NSLs had increased dramatically, expanding from 8,500 requests in 2000 to 47,000 in 2005, *IG Report I* at 120. During the three years under review, the percentage of NSLs used to investigate Americans (“U.S. persons”) increased from 39% in 2003 to 53% in 2005. A substantial majority of the requests involved records relating to telephone or e-mail communications. The report is somewhat critical of the FBI’s initial performance:

[W]e found that the FBI used NSLs in violation of applicable NSL statutes, Attorney General Guidelines, and internal FBI policies. In addition, we found that the FBI circumvented the requirements of the ECPA NSL statute when it issued at least 739 “exigent letters” to obtain telephone toll billing records and subscriber information from three telephone companies without first issuing NSLs.

The second IG Report reviewed the FBI’s use of national security letter authority during calendar year 2006 and the corrective measures taken following the issuance of the IG’s first report. The second report concluded that the FBI’s use of national security letters in 2006 continued the upward trend previously identified; the percentage of NSL requests generated from investigations of U.S. persons increased from 39% of all NSL requests in 2003 to 57% in 2006; the FBI and DOJ are committed to correcting the problems identified in *IG Report I* and have made significant progress; and it is too early to say whether the corrective measures will resolve the problems previously identified.

The third IG Report examined the FBI’s use of exigent letters and other informal means of acquiring communication service provider’s customer records in lieu of relying on NSL authority during the period from 2003 to 2007. The IG’s Office discovered that “the FBI’s use of exigent letters became so casual, routine, and unsupervised that employees of all three communications service providers sometimes generated exigent letters for FBI personnel to sign and return to them.”

## NSLs in Court

Prior to amendment, two lower federal court cases had indicated that the NSLs and practices surrounding their use were contrary to the requirements of the First Amendment. On appeal, one was dismissed as moot and the other sent back for reconsideration in light of the amendments. Following remand and amendment of the NSL statutes, the District Court for the Southern District of New York again concluded that the amended NSL secrecy requirements violated both First Amendment free speech and separation of powers principles.

The Court of Appeals was similarly disposed, but concluded that the government could invoke the secrecy and judicial review authority of the 18 U.S.C. 2709 and 18 U.S.C. 3511 in a limited but constitutionally permissible manner. It stated that

If the Government uses the suggested reciprocal notice procedure as a means of initiating judicial review, there appears to be no impediment to the Government's including notice of a recipient's opportunity to contest the nondisclosure requirement in an NSL. If such notice is given, time limits on the nondisclosure requirement pending judicial review, as reflected in *Freedman*, would have to be applied to make the review procedure constitutional. We would deem it to be within our judicial authority to conform subsection 2709(c) to First Amendment requirements, by limiting the duration of the nondisclosure requirement, absent a ruling favorable to the Government upon judicial review, to the 10-day period in which the NSL recipient decides whether to contest the nondisclosure requirement, the 30-day period in which the Government considers whether to seek judicial review, and a further period of 60 days in which a court must adjudicate the merits, unless special circumstances warrant additional time. If the NSL recipient declines timely to precipitate Government-initiated judicial review, the nondisclosure requirement would continue, subject to the recipient's existing opportunities for annual challenges to the nondisclosure requirement provided by subsection 3511(b). If such an annual challenge is made, the standards and burden of proof that we have specified for an initial challenge would apply, although the Government would not be obliged to initiate judicial review.

Given the possibility of constitutional application, the court saw no reason to invalidate Sections 2709(c) and 3511(b) in toto. The exclusive presumptions of Section 3511 cannot survive, the court declared, but the First Amendment finds no offense in the remainder of the two sections except, the court observed, "to the extent that they fail to provide for Government-initiated judicial review. The Government can respond to this partial invalidation ruling by using the suggested reciprocal notice procedure."

On remand under the procedure suggested by the Court of Appeals, the government submitted the declaration of the senior FBI official concerning the continued need for secrecy concerning the NSL. Following an *ex parte*, in camera hearing, the district court concluded the government had met its burden, but granted the plaintiff's motion for an unclassified, redacted summary of the FBI declaration.

The possibility of a conflicting view has arisen in the Ninth Circuit. A federal district court there agreed with the Second Circuit that the NSL confidentiality and judicial review provisions were constitutionally suspect. Yet it could not agree with the Second Circuit that NSL authority might be used if the confidentiality and judicial review provisions were implemented to satisfy constitutional demands. The statutory language was too clear and the congressional intent too apparent for the court to feel it could move in the opposite direction. It declared:

The statutory provisions at issue—as written, adopted and amended by Congress in the face of a constitutional challenge—are not susceptible to narrowing conforming constructions to save their constitutionality ... [I]n amending and reenacting the statute as it did, Congress was concerned with giving the government the broadest powers possible to issue NSL nondisclosure orders and preclude searching judicial review of the same ... [T]he sorts of multiple inferences required to save the provisions at issue are not only contrary to evidence of Congressional intent, but also contrary to the statutory language and structure of the statutory provisions actually enacted by Congress.

The district court also concluded that, if the confidentiality and judicial review provisions relating to Section 2709 could not survive; neither could the remainder of the section. The court, therefore, barred the government from using Section 2709’s NSL authority and from enforcing related NSL confidentiality provisions. It stayed the order pending appeal.

## **Recommendations of the President’s Review Group**

In the wake of leaks relating to the National Security Agency’s (NSA’s) purported bulk meta-data collection program, the President established a Review Group on Intelligence and Communications Technology. The Group released its report and recommendations on December 12, 2013. Several of its recommendations addressed NSLs. NSL procedures, it said, should more closely resemble those of Section 215 FISA court orders. Thus, it proposed that (1) the courts approve all NSLs except in emergency circumstances; (2) Section 215 orders be used only in international terrorism and international espionage investigations; (3) the NSL statutes be amended to track Section 215 minimization requirements; (4) both NSLs and Section 215 orders should be subject to greater oversight and public reporting requirements.

Section 215 of the USA PATRIOT Act amended the business records provisions of FISA. As amended, it authorizes FISA court orders for the production of tangible items held by individuals and private entities in certain foreign intelligence cases. Section 215 orders provide government access to business records in certain intelligence investigations; NSLs also provide government access to business records in certain intelligence investigations. FISA court judges issue Section 215 orders; FBI officials issue NSLs. The Group recommended that “that statutes that authorize the issuance of National Security Letters should be amended to permit the issuance of National Security Letters only upon a *judicial finding* that: (1) the government has reasonable grounds to believe that the particular information sought is relevant to an authorized investigation intended to protect ‘against international terrorism or clandestine intelligence activities’ and (2) like a subpoena, the order is reasonable in focus, scope, and breadth.”

Without further adjustments, the proposed Section 215-NSL symmetry would be less than perfect. Requiring judicial approval of both would be a first step in that direction. The Group, however, did not suggest that the FISA court should approve all NSLs. It readily conceded that the 60-a-day rate at which the FBI issues NSLs would overwhelm the FISA court as currently constituted. It offered several alternative solutions, including enlarging the FISA court, but endorsed none of the alternatives.

The Group would also eliminate the gap that exists between when an NSL may be issued and when a Section 215 order may be issued. Section 215 orders are available for investigations in addition to the international terrorism or international espionage inquiries that support NSL issuance under most statutes. Beyond terrorism and espionage, Section 215 orders are available to secure “foreign intelligence information” as long as it does not relate to a “U.S. person.”

Foreign intelligence information encompasses information about foreign nations and foreign entities useful for the conduct of U.S. foreign relations. The Group endeavored to create compatibility by shaving off the difference; it would allow Section 215 orders only in conjunction with international terrorism or espionage investigations.

Section 215 orders are subject to limitations as to how the information they generate may be used, stored, shared, and kept or disposed of (minimization standards). The Group considered “the oversight and minimization requirements governing the use of NSLs ... much less rigorous than those imposed in the use of [Section] 215 orders.” Consequently, it recommended that NSLs be held to Section 215 standards.

Finally, the Group made a series of recommendations with an eye to greater oversight and public disclosure. Their proposals would apply to NSLs, Section 215 orders, trap and trace orders, Section 702 orders, and orders of the kind that gave rise to the purported NSA bulk meta-data collection. It suggested as a general matter that information concerning these authorities should be available in detail to Congress and the public, consistent with the need to protect classified information. More specifically, it recommended that nondisclosure orders (gag orders) issued to communications carriers and other recipients should be limited to cases involving human safety, maintaining congenial diplomatic relations, or similar substantial governmental concerns. The Group would allow recipients to periodically disclose the number of times they had received NSLs, Section 215 orders, and the like. It also proposed that the government be required to issue regular public reports on the use of such orders.

## **Comparison of NSL Attributes**

The following table summarizes the differences among the five NSL sections: Section 1114(a)(5) of the Right to Financial Privacy Act (12 U.S.C. 3414); Sections 626 and 627 of the Fair Credit Reporting Act (15 U.S.C. 1681u, 1691v); Section 2709 of Title 18 of the *United States Code* (18 U.S.C. 2709); and Section 802 of the National Security Act (50 U.S.C. 3162).

**Table I. Profile of the Current NSL Statutes**

<b>NSL Statute</b>	<b>18 U.S.C. 2709</b>	<b>12 U.S.C. 3414</b>	<b>15 U.S.C. 1681u</b>	<b>15 U.S.C. 1681v</b>	<b>50 U.S.C. 3162</b>
Addressee	communications providers	financial institutions	consumer credit agencies	consumer credit agencies	financial institutions, consumer credit agencies, travel agencies
Certifying officials	senior FBI officials and SACs	senior FBI officials and SACs	senior FBI officials and SACs	supervisory official of an agency investigating, conducting intelligence activities relating to or analyzing int'l terrorism	senior officials no lower than Ass't Secretary or Ass't Director of agency w/ employees w/ access to classified material
Information covered	identified customer's name, address, length of service, and billing info	identified customer financial records	identified consumer's name, address, former address, place and former place of employment	all information relating to an identified consumer	all financial information relating to consenting, identified employee
Standard/purpose	relevant to an investigation to protect against int'l terrorism or clandestine intelligence activities	sought for foreign counter-intelligence purposes to protect against int'l terrorism or clandestine intelligence activities	sought for an investigation to protect against int'l terrorism or clandestine intelligence activities	necessary for the agency's investigation, activities, or analysis of int'l terrorism	necessary to conduct a law enforcement investigation, counter-intelligence inquiry or security determination
Dissemination	only per Att'y Gen. guidelines	only per Att'y Gen. guidelines	w/i FBI, to secure approval for intell. investigation, to military investigators when inform. relates to military member	no statutory provision	only to agency of employee under investigation, DOJ for law enforcement or intell. purposes, or fed. agency when clearly relevant to mission
Immunity/fees	no provisions	no provisions	fees; immunity for good faith compliance with a NSL	immunity for good faith compliance with a NSL	reimbursement; immunity for good faith compliance with a NSL

**Source:** Congressional Research Service, based on statutes cited in the table.

## **Author Contact Information**

Charles Doyle  
Senior Specialist in American Public Law  
cdoyle@crs.loc.gov, 7-6968