National Security Letters: Proposals in the 112th Congress

Charles Doyle
Senior Specialist in American Public Law

June 30, 2011

Congressional Research Service
7-5700
www.crs.gov
R41619

CRS Report for Congress
Prepared for Members and Committees of Congress

Summary

National Security Letters (NSLs) are roughly comparable to administrative subpoenas. Various intelligence agencies use them to demand certain customer information from communications providers, financial institutions, and consumer credit reporting agencies under the Right to Financial Privacy Act, the Fair Credit Reporting Act, the National Security Act, and the Electronic Communications Privacy Act.

The USA PATRIOT Act expanded NSL authority. Later reports of the Department of Justice's Inspector General indicated that (1) the FBI considered the expanded authority very useful; (2) after expansion the number of NSL requests increased dramatically; (3) the number of requests relating to Americans increased substantially; and (4) FBI use of NSL authority had sometimes failed to comply with statutory, Attorney General, or FBI policies.

Originally, the NSL statutes authorized nondisclosure requirements prohibiting recipients from disclosing receipt or the content of an NSL to anyone, ever. They now permit judicial review of these secrecy provisions. As understood by the courts, recipients may request the issuing agency to seek and justify to the court the continued binding effect of any secrecy requirement.

In conjunction with congressional consideration of three expiring USA PATRIOT Act-related amendments to the Foreign Intelligence Surveillance Act (FISA), the Senate Judiciary Committee recommended that the NSL statutes be returned to their USA PATRIOT Act form and that judicial construction of the nondisclosure provisions be codified, S.Rept. 112-13 to accompany S. 193. Thereafter, Congress extended the FISA provisions in separate legislation, P.L. 112-14 (S. 990). Senator Leahy (S. 1125) and Representative Conyers (H.R. 1805) have reintroduced the NSL proposals found in S. 193. Senator Paul has offered several proposals to require FISA court approval before an NSL could be executed as well as to require NSL minimization standards (S. 1050, S. 1070, S. 1073, and S. 1075).

This report reprints the text of the five NSL statutes as they now appear and as they appeared prior to amendment by the USA PATRIOT Act (to which form they would be returned under S. 1125 and H.R. 1805). Related reports include CRS Report R40138, *Amendments to the Foreign Intelligence Surveillance Act (FISA) Extended Until June 1, 2015*, by Edward C. Liu, and CRS Report RL33320, *National Security Letters in Foreign Intelligence Investigations: Legal Background and Recent Amendments*, by Charles Doyle.

Contents

Tables

Contacts

Introduction

National Security Letters (NSLs) are roughly comparable to administrative subpoenas. Intelligence agencies issue them for intelligence gathering purposes to telephone companies, Internet service providers, consumer credit reporting agencies, banks, and other financial institutions, directing the recipients to turn over certain customer records and similar information. The 111th Congress saw a number of proposals to amend NSL authority.[1] None were enacted, but S. 193, introduced early in the 112th Congress by Senator Leahy, would carry forward in large measure the provisions approved by the Senate Judiciary Committee in the 111th.[2]

S. 193 would also have extended three USA PATRIOT Act-related amendments to the Foreign Intelligence Surveillance Act (FISA) then scheduled to expire earlier this year.[3] The Senate Judiciary Committee reported out an amended version of S. 193 on April 6, 2011.[4] Thereafter, Congress extended the FISA amendments separately.[5] Senator Leahy then reintroduced the reported version of S. 193 as S. 1125, stripped of the FISA extension provisions. Representative Conyers introduced companion legislation in the House (H.R. 1805). Senator Paul offered several bills that address many of the same issues (S. 1050, S. 1070, S. 1073, S. 1075).

S. 1125 and H.R. 1805 would repeal one of NSL's authorizing statutes, section 627 of the Fair Credit Reporting Act (15 U.S.C. 1681v); return the others, as of December 31, 2013, to their pre-USA PATRIOT Act form; amend the judicial review procedure to reflect judicial constructions; and adjust the audit and reporting requirements. S. 1073 would require the Attorney General to issue minimization procedures for NSLs. S. 1075 would permit issuance of a NSL only upon the order of a FISA court judge. S. 1050 and S. 1070 would combine the two proposals and require minimization procedures and FISA court orders for NSLs.[6]

---

[1] See generally CRS Report R40887, *National Security Letters: Proposed Amendments in the 111th Congress*, by Charles Doyle, from which this report borrows heavily.

[2] See S. 1692 (111th Cong); S.Rept. 111-92 (2009).

[3] The so-called "lone wolf," "roving wiretap," and "section 215" amendments to FISA were scheduled to expire May 27, 2011. The temporary roving wiretap and section 215 provisions had originated in the USA PATRIOT Act, P.L. 107-56 (2001) and were first scheduled to expire on December 31, 2005. Congress extended their expiration date and that of the lone wolf provision on several occasions:

- from December 31, 2005 to February 3, 2006 (P.L. 109-160, 119 Stat. 2957(2005))
- from February 3, 2006 to March 10, 2006 (P.L. 109-170, 120 Stat. 3 (2006))
- from March 10, 2006 to December 31, 2009 (P.L. 109-177, 120 Stat. 194-95 (2006))
- from December 31, 2009 to February 28, 2010 (P.L. 111-118, 123 Stat. 3470 (2009))
- from February 28, 2010 to February 28, 2011 (P.L. 111-141, 124 Stat. 37 (2010))
- from February 28, 2011 to May 27, 2011 (P.L. 112-3, 125 Stat. 5 (2011)) and finally
- from May 27, 2011 to June 1, 2015 (P.L. 112-14, 125 Stat. 216 (2011)).

See generally, S.Rept. 112-13, at 2-12 (2011); CRS Report R40138, *Amendments to the Foreign Intelligence Surveillance Act (FISA) Extended Until June 1, 2015*, by Edward C. Liu.

[4] S.Rept. 112-13 (2011). Senator Leahy also introduced S. 290. S. 193 and S. 290, as introduced, are identical.

[5] P.L. 112-14, 125 Stat. 216 (2011).

[6] S. 1050, S. 1070, S. 1125, and H.R. 1805 also contain proposals to amend FISA that are beyond the scope of this report.

Background

Prior to the USA PATRIOT Act, the NSL statutes were four. One, 18 U.S.C. 2709, obligated communications providers to supply certain customer information upon the written request of the Director of the Federal Bureau of Investigation (FBI) or a senior FBI headquarters official.[7] When customer identity, length of service, and toll records were sought, the letters had to certify (1) that the information was relevant to a foreign counterintelligence investigation and (2) that specific and articulable facts gave reason to believe the information pertained to a foreign power or its agents.[8] When only customer identity and length of service records (but not toll records) were sought, the letters had to certify (1) again that the information was relevant to a foreign counterintelligence investigation, but (2) that specific and articulable facts gave reason to believe that the customer information pertained to use of the provider's facilities to communicate with foreign powers, their agents, or those engaged in international terrorism or criminal clandestine intelligence activities.[9]

In like manner a second statute, Section 1114(a)(5) of the Right to Financial Privacy Act, obligated financial institutions to provide the FBI with customers' financial records upon written certification of the FBI Director or his designee (1) that the records were sought for foreign counterintelligence purposes and (2) that specific and articulable facts gave reason to believe that the records were those of a foreign power or its agents.[10]

And so it was with a third, Section 626 of the Fair Credit Report Act, which obligated consumer credit reporting agencies to provide customer identification, and the names and addresses of financial institutions at which a designated consumer maintained accounts.[11] Here too, the obligation was triggered by written certification of the FBI Director or his designee (1) that the information was necessary for a foreign counterintelligence investigation, and (2) that specific and articulable facts gave reason to believe that the consumer was either a foreign power, a foreign official, or the agent of a foreign power and was engaged in international terrorism or criminal clandestine intelligence activities.[12]

The fourth, Section 802 of the National Security Act, was a bit different.[13] It reached a wider range of potential recipients at the demand of a large group of federal officials, but for a more limited purpose. It rested the obligation to provide consumer reports, together with financial information and records, upon consumer reporting agencies, financial agencies, and financial institutions, or holding companies.[14] The requirement was triggered by the certification of senior officials of law enforcement and intelligence agencies, but confined to information pertaining to

[7] 18 U.S.C. 2709(a), (b) (2000 ed.).

[8] 18 U.S.C. 2709(b)(1) (2000 ed.).

[9] 18 U.S.C. 2709(b)(2) (2000 ed.).

[10] 12 U.S.C. 3414(a)(5) (2000 ed,).

[11] 15 U.S.C. 1681u(a), (b) (2000 ed.).

[12] Id.

[13] 50 U.S.C. 436 (2000 ed.).

[14] Id.

federal employees with access to classified information and being sought for clearance purposes and inquiries into past or potential security leaks.[15]

USA PATRIOT Act

Section 505 of the USA PATRIOT Act altered the FBI's NSL authority under Section 2709, the Right to Financial Privacy Act, and the Fair Credit Reporting Act in several ways:

- it expanded issuing authority to include the heads of FBI field offices (special agents in charge (SACs));
- it eliminated the requirement of specific and articulable facts demonstrating a nexus to a foreign power or its agents;
- it required instead that the information was sought for or relevant to various national security investigations; and
- it directed that no NSL related investigation of a "U.S. person" (American citizen or foreign resident alien) be predicated exclusively on First Amendment protected activities.[16]
- The National Security Act NSL section remained unchanged, but Section 358(g) of the USA PATRIOT Act added a new Fair Credit Reporting Act NSL Section 627, 15 U.S.C. 1681v. The new section obligated consumer reporting agencies to provide consumer information and reports to a federal agency "authorized to conduct investigations of, or intelligence or counterintelligence activities or analysis related to, international terrorism."[17] Senior federal agency officials were empowered to issue the NSL with a certification that the information was "necessary for the agency's conduct or such investigation, activity, or analysis."[18]

[15] Id.

[16] Thus for example, section 626 of the Fair Credit Report Act, once stated in part that:

> The Director or the Director's designee may make such a certification only if [he or she] has determined in writing that—(1) such information is necessary for the conduct of an authorized foreign counterintelligence investigation; and (2) there are specific and articulable facts giving reason to believe that the consumer—(A) is a foreign power ... or a person who is not a United States person ... and is an official of a foreign power; or (b) is an agent of a foreign power and is engaging or has engaged in an act of international terrorism ... or clandestine intelligence activities that involve or may involve a violation of criminal statutes of the United States, 15 U.S.C. 1681u(a) (2000 ed.).

The USA PATRIOT Act redesignated section 626 as section 625 and the amended provision stated that:

> The Director or the Director's designee in a position not lower than Deputy Assistant Director at Bureau headquarters or Special Agent in Charge of a Bureau field office designated by the Director may make such a certification only if [he or she] has determined in writing that such information is sought for the conduct of an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States, U.S.C. 1681u(a)(2000 ed. Supp.I).

[17] 15 U.S.C. 1681v(a)(2000 ed. Supp. I).

[18] Id.

2006 Amendments

Several of the USA PATRIOT Act's intelligence gathering provisions were temporary and originally set to expire after five years.[19] The NSL statutes were not among them, but Congress amended the statutes in the USA PATRIOT Improvement and Reauthorization Act of 2005 and the USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006 nonetheless.[20] The NSL statute amendments were driven both by sensitivity to an Administration desire for more explicit enforcement authority[21] and by judicial developments which had raised questions as to the statutes' constitutional vitality as then written.[22] The statutes then came with open-ended nondisclosure provisions which barred recipients from disclosing the fact or content of the NSL—ever or to anyone. Yet, they featured neither a penalty provision should the confidential requirement be breached nor in most cases an enforcement mechanism should an NSL obligation be ignored (the original Fair Credit Report Act statute alone had an explicit judicial enforcement component).

The amendments:

- created a judicial enforcement mechanism and a judicial review procedure for both the requests and accompanying nondisclosure requirements;[23]
- established specific penalties for failure to comply with the nondisclosure requirements;[24]
- made it clear that the nondisclosure requirements did not preclude a recipient from consulting an attorney;[25]
- provided a process to ease the nondisclosure requirement;[26]
- expanded congressional oversight;[27] and
- called for Inspector General's audits of use of NSL authority.[28]

[19] Sec. 224, P.L. 107-56, 115 Stat. 295 (2001).

[20] P.L. 109-177, 120 Stat. 192 (2006); P.L. 109-178, 120 Stat. 278 (2006), respectively.

[21] E.g., Anti-Terrorism Intelligence Tools Improvement Act of 2003: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security, 108th Cong., 2d Sess. 7-8 (2004)(prepared statement of U.S. Ass't Att'y Gen. Daniel J. Bryant).

[22] *Doe v. Ashcroft*, 334 F.Supp.2d 471 (S.D.N.Y. 2004)(First and Fourth Amendment concerns); *Doe v. Gonzales*, 386 F.Supp.2d 66 (D. Conn. 2005)(First Amendment concerns).

[23] 28 U.S.C. 3511.

[24] 28 U.S.C. 3511(c), 18 U.S.C. 1510(e).

[25] 12 U.S.C. 3414((a)(3)(A); 15 U.S.C. 1681v(c)(1), 1681u(d)(1); 18 U.S.C. 2709(c)(1); 50 U.S.C. 436(B)(1).

[26] 28 U.S.C. 3511(b).

[27] P.L. 109-177, §118.

[28] P.L. 109-177, §119.

IG Reports

The First IG Report

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.[29] 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.[30] A substantial majority of the requests involved records relating to telephone or e-mail communications, Id.

The report and the subsequent report a year later provided a glimpse at how the individual NSL statutes were used and why they were considered valuable. In case of the 18 U.S.C. 2709, the Electronic Communications Privacy Act (ECPA) NSL statute, the reports explained that:

> Through national security letters, an FBI field office obtained telephone toll billing records and subscriber information about an investigative subject in a counterterrorism case. The information obtained identified the various telephone numbers with which the subject had frequent contact. Analysis of the telephone records enabled the FBI to identify a group of individuals residing in the same vicinity as the subject. The FBI initiated investigations on these individuals to determine if there was a terrorist cell operating in the city.[31]
>
> Headquarters and field personnel told us that the principal objective of the most frequently used type of NSL – ECPA NSLs seeking telephone toll billing records, electronic communication transactional records, or subscriber information (telephone and e-mail) – is to develop evidence to support applications for FISA orders.[32]

The Right to Financial Privacy Act (RFPA) NSL statute, 12 U.S.C. 3414(a)(5), also affords authorities access to a wide range of information (bank transaction records v. telephone transaction records) as demonstrated by the instances where it proved useful:

> The FBI conducted a multi-jurisdictional counterterrorism investigation of convenience store owners in the United States who allegedly sent funds to known Hawaladars (persons who use the Hawala money transfer system in lieu of or parallel to traditional banks) in the Middle East. The funds were transferred to suspected Al Qaeda affiliates. The possible violations

[29] U.S. Department of Justice, Office of the Inspector General, *A Review of the Federal Bureau of Investigation's Use of National Security Letters* (*IG Report I*) (March 2007); *A Review of the FBI's Use of National Security Letters: Assessment of Corrective Actions and Examination of NSL Usage in 2006* (*IG Report II*) (March 2008*); A Review of the Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records* (*IG Report III*), all three available at http://www.usdoj.gov/oig/special/index.htm.

[30] *Id.* A "U.S. person" is generally understood to mean "a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101(a)(2) of title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection(a)(1), (2), or (3) of this section," 50 U.S.C. 1801.

[31] *IG Report I* at 49.

[32] *IG Report II* at 65. The Foreign Intelligence Surveillance Act (FISA) authorizes the FBI to apply for court orders in national security cases authorizing electronic surveillance, physical searches, the installation and use of pen registers and trap and trace devices, and access to business records and other tangible property, 50 U.S.C. 1801-1862.

> committed by the subjects of these cases included money laundering, sale of untaxed cigarettes, check cashing fraud, illegal sale of pseudoephedrine (the precursor ingredient used to manufacture methamphetamine), unemployment insurance fraud, welfare fraud, immigration fraud, income tax violations, and sale of counterfeit merchandise.[33]
>
> The FBI issued national security letters for the convenience store owners' bank account records. The records showed that two persons received millions of dollars from the subjects and that another subject had forwarded large sums of money to one of these individuals. The bank analysis identified sources and recipients of the money transfers and assisted in the collection of information on targets of the investigation overseas.[34]

The Fair Credit Reporting Act NSL statutes, 15 U.S.C. 1681u (FCRAu) and 1681v (FCRAv) can be even more illuminating: "The supervisor of a counterterrorism squad told us that the FCRA NSLs enable the FBI to see 'how their investigative subjects conduct their day-to-day activities, how they get their money, and whether they are engaged in white collar crime that could be relevant to their investigations.'"[35]

Overall, the report notes that the FBI used the information gleaned from NSLs for a variety of purposes, "to determine if further investigation is warranted; to generate leads for other field offices, Joint Terrorism Task Forces, or other federal agencies; and to corroborate information developed from other investigative techniques."[36] Moreover, information supplied in response to NSLs provides the grist of FBI analytical intelligence reports and various FBI databases.[37]

The report was somewhat critical, however, 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. Moreover, in a few other instances, the FBI sought or obtained telephone toll billing records in the absence of a national security investigation, when it sought and obtained consumer full credit reports in a counterintelligence investigation, and when it sought and obtained financial records and telephone toll billing records without first issuing NSLs. *Id.* at 124.

More specifically, the report found that:

- a "significant number of NSL-related possible violations were not being identified or reported" as required;
- the only FBI data collection system produced "inaccurate" results;
- the FBI issued over 700 exigent letters acquiring information in a manner that "circumvented the ECPA NSL statute and violated the Attorney General's Guidelines ... and internal FBI policy;"

[33] Critics might suggest that these offenses are "possible" in the operation of any convenience store.

[34] *IG Report I* at 50.

[35] *Id.* at 51.

[36] *Id.* at 65.

[37] Id.

- the FBI's Counterterrorism Division initiated over 300 NSLs in a manner that precluded effective review prior to approval;
- 60% of the individual files examined showed violations of FBI internal control policies;
- the FBI did not retain signed copies of the NSLs it issued;
- the FBI had not provided clear guidance on the application of the Attorney General's least-intrusive-feasible-investigative-technique standard in the case of NSLs;
- the precise interpretation of toll billing information as it appears in the ECPA NSL statute is unclear;
- SAC supervision of the attorneys responsible for review of the legal adequacy of proposed NSLs made some of the attorneys reluctant to question the adequacy of the underlying investigation previously approved by the SAC;
- there was no indication that the FBI's misuse of NSL authority constituted criminal conduct;
- personnel both at FBI headquarters and in the field considered NSL use indispensable; and
- information generated by NSLs was fed into a number of FBI systems. *IG Report I* at 121-24.

Exigent Letters

Prior to enactment of the Electronic Communications Privacy Act (ECPA), the Supreme Court held that customers had no Fourth Amendment protected privacy rights in the records the telephone company maintained relating to their telephone use.[38] Where a recognized expectation of privacy exists for Fourth Amendment purposes, the Amendment's usual demands such as those of probable cause, particularity, and a warrant may be eased in the face of exigent circumstances. For example, the Fourth Amendment requirement that officers must knock and announce their purpose before forcibly entering a building to execute a warrant can be eased in the presence of certain exigent circumstances such as the threat of the destruction of evidence or danger to the officers.[39] Satisfying Fourth Amendment requirements, however, does not necessarily satisfy statutory prohibitions.

The ECPA prohibits communications service providers from supplying information concerning customer records unless one of the statutory exceptions applies.[40] There are specific exceptions for disclosure upon receipt of a grand jury subpoena[41] or an NSL.[42] A service provider who

[38] *Smith v. Maryland*, 442 U.S. 735, 745 (1979)

[39] *Richards v. Wisconsin*, 520 U.S. 385, 391 (1997); *Wilson v. Arkansas*, 514 U.S. 927, 936 (1995).

[40] 18 U.S.C. 2702(c).

[41] 18 U.S.C. 2703(c)(2).

[42] 18 U.S.C. 2709(a).

knowingly or intentionally violates the prohibition is subject to civil liability,[43] but there are no criminal penalties for the breach.

The Inspector General found that contrary to assertions that "the FBI would obtain telephone records only after it served NSLs or grand jury subpoenas, the FBI obtained telephone bill records and subscriber information prior to serving NSLs or grand jury subpoenas" by using "exigent letters."[44] The FBI responded that it had barred the use of exigent letters, but emphasized that the term "exigent letter" does not include emergency disclosures under the exception now found in 18 U.S.C. 2702(c)(4). Thus, the FBI might request that a service provider invoke that exception to the record disclosure bar "if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information," 18 U.S.C. 2702(c)(4). Moreover, the Justice Department's Office of Legal Counsel subsequently advised the FBI in a classified memorandum that "under certain circumstances the ECPA does not prohibit electronic communications service providers from disclosing certain call detail records to the FBI on a voluntary basis without legal process or a qualifying emergency under Section 2702."[45]

The Second IG Report

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 ... identified ... for the period covering 2003 through 2006;
- "the percentage of NSL requests generated from investigations of U.S. persons continued to increase significantly, from approximately 39% of all NSL requests issued in 2003 to approximately 57% of all NSL requests issued in 2006;"
- the FBI and DOJ are committed to correcting the problems identified in *IG Report I* and "have made significant progress in addressing the need to improve compliance in the FBI's use of NSLs;" [and]
- "it [was] too early to definitively state whether the new systems and controls developed by the FBI and the Department will eliminate fully the problems with NSLs that we identified," *IG Report II* at 8-9.

[43] 18 U.S.C. 2707(a).

[44] *IG Report I* at 90.

[45] *Report by the Office of the Inspector General of the Department of Justice on the Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the House Comm. on the Judiciary*, 111th Cong. 2d sess. 22 (2010) (*2010 Hearings*) (statement of Department of Justice Inspector General Glenn Fine)(referring to a January, 2010 OLC memorandum).

The Third IG Report

The third IG Report examined the FBI's use of exigent letters and other informal means of acquiring communication service providers' customer records in lieu of relying on NSL authority during the period from 2003 to 2007.[46] 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."[47]

Some of the informality was apparently the product of proximity. In order to facilitate cooperation, communications providers had assigned employees to FBI offices. In addition to a relaxed exigent letter process, the on-site feature gave rise to a practice of sneak peeks, that is, of providing the FBI with "a preview of the available information for a targeted phone number, without documentation of any justification for the request."[48] "In fact, at times the service providers' employees simply invited FBI personnel to view the telephone records on their computer screens. One senior FBI counterterrorism official described the culture of casual requests for telephone records by observing, 'It [was] like having the ATM in your living room.'"[49]

Not surprisingly, the IG's review

> found widespread use by the FBI of exigent letters and other informal requests for telephone records. These other requests were made ... without first providing legal process or even exigent letters. The FBI also obtained telephone records through improper 'sneak peeks,' community of interest [redacted], and hot-number [redacted] Many of these practices violated FBI guidelines, Department policy, and the ECPA statute. In addition, we found that the FBI also made inaccurate statements to the FISA Court related to its use of exigent letters.[50]

Although critical of the FBI's initial response and recommending further steps to prevent reoccurrence, the IG's Report concluded that "the FBI took appropriate action to stop the use of exigent letters and to address the problems created by their use."[51]

[46] *IG Report III* at 1.

[47] *2010 Hearings* at 14 (statement of Department of Justice Inspector General Glenn Fine)

[48] *Id.* at 15.

[49] *Id.*

[50] *Id.* at 288 (redaction in the original).

[51] *IG Report III* at 289.

Table 1. Profile of the Current NSL Statutes

NSL statute	18 U.S.C. 2709	12 U.S.C. 3414	15 U.S.C. 1681u	15 U.S.C. 1681v	50 U.S.C. 436
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 relating to 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 an NSL	immunity for good faith compliance with an NSL	reimbursement; immunity for good faith compliance with an NSL

Secrecy, Judicial Review, and the Second Circuit

The current secrecy and judicial review provisions applicable to NSLs must be read in light of the Second Circuit's *John Doe, Inc. v. Mukasey* decision, 549 F.3d 861 (2d Cir. 2008). Under the NSL statutes, secrecy is not absolutely required. Instead, NSL recipients are bound to secrecy only upon the certification of the requesting agency that disclosure of the request or response may result in a danger to national security; may interfere with diplomatic relations or with a criminal, counterterrorism, or counterintelligence investigation; or may endanger the physical safety of an

individual.[52] A recipient may disclose the request to those necessary to comply with the request and to an attorney the recipient consults for related legal advice or assistance.[53] In doing so, the recipient must advise them of the secrecy requirements.[54] Aside from its attorney the recipient must also identify, at the requesting agency's election, those to whom it has disclosed the request.[55]

Judicial Review of NSLs

Under the statute, 18 U.S.C. 3511, *a recipient may petition the court to modify or extinguish any NSL secrecy requirement* within a year of issuance.[56] Thereafter, it may petition to have the veil of secrecy lifted, although it may resubmit a rejected request only once a year.[57] Section 3511 provides that the court may modify or set aside the restriction if it finds "no reason to believe that disclosure may" endanger national security or personal safety or interfere with diplomatic relations or a criminal, counterterrorism, or counterintelligence investigation.[58] The section, however, *binds the court to the assertion of a senior executive branch official that such an adverse consequence is possible*.[59]

In addition to authority to review and set aside NSL nondisclosure requirements, the federal courts also enjoy jurisdiction to review and enforce the underlying NSL requests. Under Section 3511, recipients may petition and be granted an order modifying or setting aside an NSL, if the court finds that compliance would be unreasonable, oppressive, or otherwise unlawful.[60] The "unreasonable or oppressive" standard is used for grand jury and other subpoenas issued under the Federal Rules of Criminal Procedure.[61] The Rules afford protection against undue burdens and protect privileged communications.[62] Compliance with a particular NSL might be unduly burdensome in some situations, but the circumstances under which NSLs are used suggest few federally recognized privileges. The Rules also impose a relevancy requirement, but in the context of a grand jury investigation a motion to quash will be denied unless it can be shown that "there is no reasonable possibility that the category of materials the Government seeks will produce information relevant" to the investigation.[63] The authority to modify or set aside an NSL that is "unlawful" affords the court an opportunity to determine whether the NSL in question complies with the statutory provisions under which it was issued. Section 3511 also vests the court with authority to enforce the NSL against a recalcitrant recipient. Failure to comply with the court's order thereafter is punishable as contempt of court.[64] A breach of a confidentiality

[52] *E.g.*, 18 U.S.C. 2709(c)(1). The other NSL statutes have comparable provisions.

[53] Id.

[54] *E.g.*, 12 U.S.C. 3414(a)(5)(D)(iii). The other NSL statutes have comparable provisions.

[55] *E.g.*, 15 U.S.C. 1681u(d)(4). The other NSL statutes have comparable provisions.

[56] 18 U.S.C. 3511(b)(2). As explained below, the Second Circuit opinion requires that the provisions in italics here and at the end of the paragraph be understood in the context of First Amendment demands.

[57] 18 U.S.C. 3511(b)(3).

[58] 18 U.S.C. 3511(b)(2), (3).

[59] Id.

[60] 18 U.S.C. 3511(a).

[61] F.R.Crim.P. 17(c)(2).

[62] 2 WRIGHT, FEDERAL PRACTICE AND PROCEDURE §275 (Crim. 3d ed. 2000).

[63] *United States v. R. Enterprises, Inc.*, 498 U.S. 292, 301 (1991).

[64] 18 U.S.C. 3511(c).

requirement committed knowingly and with the intent to obstruct an investigation or related judicial proceedings is punishable by imprisonment for not more than five years and/or a fine of not more than $250,000 (not more than $500,000 for an organization).[65]

The Second Circuit has concluded that the procedure can survive First Amendment scrutiny only if it involves the following:

- notice to NSL recipients that they may contest any secrecy order;
- expeditious government petition for judicial review of a secrecy order upon recipient request;
- government burden to establish the validity of its narrowly tailored secrecy order;
- no conclusive weight may be afforded governmental assertions; and
- recipients may apply or reapply annually for judicial review where the government's burden remains the same.[66]

On remand, the district upheld continuation of the nondisclosure order under the procedure suggested by the Second Circuit.[67]

Proposed Amendments

Sunset and Repeal

Three provisions governing foreign intelligence investigations sunset on June 1, 2015. The NSL provisions are not among them. None of the NSL statutes are scheduled to expire. S. 1125 and H.R. 1805 would change that. They would repeal Section 627 effective December 31, 2013, and on that date would return the others to their pre-USA PATRIOT Act form.[68] They would establish a transition provision under which the law prior to December 31, 2013, would continue to apply with respect to investigations or offenses begun prior to that date.[69]

The USA PATRIOT Act expanded existing authority under 18 U.S.C. 2709, the Right to Financial Privacy Act, and the Fair Credit Reporting Act.[70] It also created new NSL authority in the form of Section 627 of the Fair Credit Reporting Act (15 U.S.C. 1681v).[71] It did not expand the reach of

[65] 18 U.S.C. 1510(e), 3571, 3559.

[66] *John Doe, Inc. v. Mukasey*, 549 F.3d 861, 883-84 (2d Cir. 2008).

[67] *Doe v. Holder*, 640 F.Supp. 2d 517 (S.D.N.Y. 2009); see also *Doe v. Holder*, 665 F.Supp. 2d 426 (S.D.N.Y. 2009)(finding continued compliance with the nondisclosure order justified); *Doe v. Holder*, 703 F.Supp.2d 313 (S.D.N.Y. 2010)(permitting the disclosure of some related information).

[68] S. 1125, §2(a)(1); H.R. 1805, §2(c)(1). The text of the NSL statutes, now and in the form to which they would be returned, is appended.

[69] S. 1125, §2(c)(2)("Notwithstanding paragraph (1), the provisions of law referred to in paragraph (1), as in effect on December 30, 2013, shall continue to apply on and after December 31, 2013, with respect to any particular foreign intelligence investigation or with respect to any particular offense or potential offense that began or occurred before December 31, 2013"); H.R. 1805, §2(c)(2)(same language).

[70] P.L. 107-56, §505, 115 Stat. 365 (2001).

[71] P.L. 107-56, §358(g), 115 Stat. 327 (2001).

the National Security Act NSL statute. A return to the state of the law prior to enactment of the USA PATRIOT Act would have the effect of eliminating the amendments it made in the pre-existing NSL statutes as well as any subsequent amendments, and of repealing Section 627.

In general terms for the three pre-existing NSL statutes, the USA PATRIOT Act:

- expanded issuing authority to include the heads of FBI field offices (special agents in charge (SACs));
- eliminated the requirement of specific and articulable facts demonstrating a nexus to a foreign power or its agents;
- required instead that the information was sought for or relevant to various national security investigations; and
- directed that no NSL related investigation of a "U.S. person" (American citizen or foreign resident alien) be predicated exclusively on First Amendment protected activities.[72]

This means that:

- NSLs are more readily available to FBI field agents at a lower level of supervisory control;
- NSLs can be used to obtain information pertaining to individuals two, three, or more steps removed from the foreign power or agent of a foreign power that is the focus of the investigation; and
- NSL-related investigations may not be predicated solely on the basis of activities protected by the First Amendment.

A return to the state of the law prior to the effective date of the USA PATRIOT Act would mean that NSLs would need to be approved by the FBI Director or a senior FBI headquarters official, and they would have to be based on specific and articulable facts giving reason to believe that the information sought pertains to a foreign power or agent of a foreign power.[73] A witness at an earlier congressional hearing indicated that the "specific and articulable" facts standard grew out of the standards employed in counterintelligence investigations and did not always translate well in a counterterrorism context:

> My point is that the "specific and articulable facts" standard was particularly suited to the counterintelligence operations of the era in which it was created. A FBI counterintelligence investigation involved examining a linear connection between a foreign intelligence officer (about whom much was known) and his contacts (potential spies). The information known about the intelligence officer was specific in nature, and could be readily used to meet the NSL legal standards.... Unlike the traditional linear counterintelligence case, in which the foreign agent tried to recruit the domestic spy using infrequent and highly secure forms of communication, many counterterrorism cases involved complex networks generating a much larger volume of communication and financial transactions. In counter-terrorism cases, the starting point was often not a clearly identifiable agent of a foreign power (as in counterintelligence); indeed, the relevant "foreign power" was itself an imperfectly

[72] 18 U.S.C. 2709((b), 12 U.S.C. 3414(a)(5)(A), 15 U.S.C. 1681u(a).

[73] 18 U.S.C. 2709((b)(2000 ed.), 12 U.S.C. 3414(a)(5)(A)(2000 ed.), 15 U.S.C. 1681u(a)(2000 ed.).

> understood terrorist organization that might defy precise definition. As a consequence, counter-terrorism investigators often had a far more difficult time meeting the "specific and articulable facts" standard.[74]

The language precluding NSL-related investigations grounded exclusively on the exercise of First Amendment rights would also have disappeared. It is at best unclear, however, that the First Amendment unaided does not embody a comparable prohibition.

Prior to the USA PATRIOT Act, the NSL statutes strictly prohibited recipients from disclosing the request to anyone, ever.[75] Yet, they afforded recipients no explicit means to challenge or seek limited release from the nondisclosure requirement,[76] even for such narrow purposes as consulting their attorneys for advice on their obligations to comply. On the other hand, they provided the FBI with no explicit remedy should recipients violate the nondisclosure requirement.

In the USA PATRIOT Improvement and Reauthorization Act, Congress addressed the issue in three ways. First, it amended the federal obstruction of justice statute to outlaw unjustified disclosures.[77] Second, it amended the NSL statutes to make it clear that a recipient remained free to seek the advice of counsel before complying.[78] These amendments, unlike the obstruction of justice amendment, would disappear should the NSL statutes return to their earlier versions. Congress's third response, however, would mitigate impact of the disappearance. Third, Congress created a nonexpiring statutory section for review of NSLs, 18 U.S.C. 3511.

By and large, Section 3511 governs judicial review of NSL nondisclosure requirements. When implemented as required by the Second Circuit's decision in *John Doe, Inc. v. Mukasey*, 549 F.3d 861 (2d Cir. 2008), and at the election of the recipient, the government has the burden of persuading the court of the validity of the gag order under the same standards as found in the expired portions of the NSL statutes. Although S. 1125 and H.R. 1805 would amend Section 3511, they each reinforce rather than erode the recipient protections of Section 3511 as discussed *infra*.

Section 627, the NSL statute created in the USA PATRIOT Act, is arguably the most sweeping of the NSL statutes. It offers the most extensive array of information (all information pertaining to a consumer held by a consumer credit reporting agency) to the widest range of requesters (any federal agency "authorized to conduct investigations of, or intelligence or counterintelligence activities or analysis relating to, international terrorism").[79] Its repeal might be seen to facilitate

---

[74] *National Security Letters: The Need for Greater Accountability and Oversight: Hearing Before the Senate Comm. on the Judiciary*, 110th Cong., 2d sess. (2008)(testimony of Michael J. Woods, former Chief of the FBI's National Security Law Unit), available on Oct. 23, 2009 at [http://judiciary.senate.gov/pdf/08-04-23WoodsTestimony.pdf].

[75] 12 U.S.C. 3414(a)(5)(D)(2000 ed.); 15 U.S.C. 1681u(d)(2000 ed.); 18 U.S.C. 2709(c)(2000 ed.); 50 U.S.C. 436(b) (2000 ed.).

[76] Depending upon one's perspective these provisions may be described as nondisclosure provisions, secrecy provisions, or gag order provisions. The descriptions are used interchangeably without any intended connotations in this report.

[77] 18 U.S.C. 1510(e).

[78] 12 U.S.C. 3414(a)(5)(D); 15 U.S.C. 1681u(d); 18 U.S.C. 2709(c); 50 U.S.C. 436(b).

[79] 15 U.S.C. 1681v(a). Such agencies would presumably include at a minimum those agencies who are members of the "intelligence community," see e.g., 50 U.S.C. 401a(4)("The term 'intelligence community' includes the following: (A) The Office of the Director of National Intelligence. (B) The Central Intelligence Agency. (C) The National Security Agency. (D) The Defense Intelligence Agency. (E) The National Geospatial-Intelligence Agency. (F) The National Reconnaissance Office. (G) Other offices within the Department of Defense for the collection of specialized national (continued...)

oversight, since it would centralize authority to issue NSLs in the FBI (other than in the case of employee security investigations under the National Security Act). Moreover, the Justice Department IG reported that both the FBI and consumer reporting agencies had experienced difficulty distinguishing between authority under 1681u and 1681v.[80]

In contrast, the National Security Act NSL statute, left unamended by the USA PATRIOT Act, is arguably the least intrusive. It reaches only information pertaining to federal employees who have consented to their disclosure.[81]

The Minority Views in the Senate Judiciary Committee report objected to a return of the NSL statutes to their earlier versions:

> S. 193 rescinds these valuable tools by, starting in 2013, requiring the government to follow the cumbersome pre-PATRIOT Act NSL standard. Prior to the PATRIOT Act, not only did the requested records have to be relevant to an investigation, but the FBI also had to have specific and articulable facts giving reason to believe that the information requested pertained to a foreign power or an agent of a foreign power, such as a terrorist or spy. This pre-PATRIOT Act requirement kept the FBI from using NSLs to develop evidence at the early stages of an investigation, which is precisely when they are the most useful, and often prevented investigators from acquiring records that were relevant to an ongoing international terrorism or espionage investigation.
>
> It makes little sense to roll back the sensible NSL reforms that were made as part of the USA PATRIOT Act. Criminal investigators have long been able to use administrative or grand jury subpoenas to obtain records, so long as they are relevant to their investigation.[82]

Nondisclosure

Each of the NSL statutes has a nondisclosure provision.[83] They state that the issuing agency may prohibit recipients from disclosing the request—to anyone other than their attorney and those necessary to comply with the request, ever.[84] In order to activate the authority, agency officials must certify that disclosure may endanger national security, endanger individual safety, or may

(...continued)

intelligence through reconnaissance programs. (H) The intelligence elements of the Army, the Navy, the Air Force, the Marine Corps, the Federal Bureau of Investigation, and the Department of Energy. (I) The Bureau of Intelligence and Research of the Department of State. (J) The Office of Intelligence and Analysis of the Department of the Treasury. (K) The elements of the Department of Homeland Security concerned with the analysis of intelligence information, including the Office of Intelligence of the Coast Guard. (L) Such other elements of any other department or agency as may be designated by the President, or designated jointly by the Director of National Intelligence and the head of the department or agency concerned, as an element of the intelligence community"). Admittedly, section 1681v only identifies those who may invoke NSL authority, not necessarily those who have or will exercise that authority.

[80] *IG Report I*, at 80-1, 125; *IG Report II*, at 29-30.

[81] 50 U.S.C. 436(a)(3)(A).

[82] S.Rept. 112-13, at 41-2 (2011)(Minority Views). Although they are both available in terrorism investigations, NSLs and grand jury subpoenas are not completely analogous, for example recipients of grand jury subpoenas are not ordinarily bound by the grand jury secrecy rules, see e.g., F.R.Crim.P. 6(e)(2)(A)("No obligation of secrecy may be imposed on any person except in accordance with Rule 6(e)(2)(B)"); *United States v. Sells Engineering, Inc.*, 463 U.S. 418, 425 (1983)("Witnesses are not under the prohibition unless they also happen to fit into one of the enumerated classes [i.e., grand juror, interpreter, court reporter, attorney for the government, and the like]"); *Butterworth v. Smith*, 494 U.S. 624 (1990)(holding unconstitutional, as a violation of the First Amendment, a Florida statute that prohibited a witness from ever disclosing his or her grand jury testimony).

[83] 12 U.S.C. 3414(a)(5)(D); 18 U.S.C. 2709(c); 15 U.S.C. 1681u(d); 15 U.S.C. 1681v(c); 50 U.S.C. 436(b).

[84] Id.

interfere with diplomatic relations or with a criminal, counterintelligence, or counterterrorism investigation.[85]

The statutes declare that a federal district court may modify or set aside an NSL secrecy requirement on the petition of a recipient, if it concludes that there is no reason to believe that disclosure might result in any such danger or interference.[86] If the petition for review is filed more than a year after issuance of the NSL, the agency must either terminate the gag order or recertify the need for its continuation.[87] They make no explicit provision for disclosure to the party to whom the information pertains.

The Second Circuit in *John Doe, Inc. v. Mukasey* held that these provisions only survive First Amendment scrutiny if the agency petitions for judicial review and convinces the court that the agency proposed order is narrowly crafted to meet to the statutorily identified adverse consequences of disclosure.[88]

S. 1125 and H.R. 1805 would modify the statutory provisions governing the issuance and judicial review of NSL nondisclosure orders. It would codify a procedure comparable in many respects to that which the Second Circuit identified as constitutionally acceptable. The agency issuing the NSL would have made the initial determination of whether to include a nondisclosure provision in the NSL and that determination would be subject to judicial review.[89] It would leave unchanged the concerns a requesting official might rely upon in order to impose a nondisclosure order: reason to believe disclosure may endanger national security or individual safety or interfere with diplomatic relations or a criminal, counterterrorism, or counterintelligence investigation.[90]

The agency would have to notify the recipient of the right to judicial review and petition for review within 30 days of a recipient's request for judicial review.[91] The agency's application for judicial approval or review would have to include a statement of facts giving reason to believe that disclosure might result in one of the statutory list of adverse consequences – endanger national security or individual safety or interfere with diplomatic relations or with a criminal, counterterrorism, or counterintelligence investigation.[92] Should the court feel the agency had met its burden after giving agency certification "substantial weight," it would be required to issue a nondisclosure order.[93]

S. 1125 and H.R. 1805 would amend each of the NSL statutes to require agency certifying officials to place a written statement in the agency's records documenting the specific facts that support the belief that the information sought in the NSL is relevant to a qualified investigation.[94]

---

[85] Id.

[86] 18 U.S.C. 3511(b)(1), (2).

[87] 18 U.S.C. 3511(b)(1), (3).

[88] 549 F.3d 861, 883 (2d Cir. 2008).

[89] S. 1125, §5 and H.R. 1805, §5; proposed 18 U.S.C. 2709(c)(1); 15 U.S.C. 1681u(d)(1); 15 U.S.C. 1681v(c)(1); 12 U.S.C. 3414(a)(5)(D); 50 U.S.C. 436(b)(1).

[90] S. 1125, §5 and H.R. 1805, §5; proposed 18 U.S.C. 2709(c)(1)(B); 15 U.S.C. 1681u(d)(1)(B); 15 U.S.C. 1681v(c)(1)(B); 12 U.S.C. 3414(a)(5)(D)(i)(II); 50 U.S.C. 436(b)(1)(B).

[91] S. 1125, §6(b) and H.R. 1805, §6(b); proposed 18 U.S.C. 3511(b)(1).

[92] S. 1125, §6(b) and H.R. 1805, §6(b); proposed 18 U.S.C. 3511(b)(2).

[93] S. 1125, §6(b) and H.R. 1805, §6(b); proposed 18 U.S.C. 3511(b)(3).

[94] S. 1125, §7 and H.R. 1805, §7; proposed 18 U.S.C. 2709(c); 15 U.S.C. 1681u(d); 15 U.S.C. 1681v(b)(2); 12 U.S.C. (continued...)

Minimization Requirements

Minimization is one of the ways that legislation in the 112th Congress differs from the legislation approved by the Senate Judiciary Committee in the previous Congress. S. 1125 and H.R. 1805 do not mention minimization. The change is apparently a response to intervening Justice Department action.[95] Senator Paul's bills include specific NSL minimization proposals.[96]

"Minimization," in this context, refers to limitations on what information is acquired; how it is acquired; how it is maintained; who has access to it within the capturing agency and under what circumstances; to whom and under what circumstances it is disclosed beyond the capturing agency; how long it is preserved; and when and under what circumstances it is expunged. Minimization standards are drawn with an eye to the purposes for which information is acquired; the authority under which it is acquired; the legitimate interests which may be affected by its acquisition, use, or disclosure; and the governmental interests served by its acquisition, maintenance, use, and disclosure.

Minimization standards ordinarily reinforce statutory and regulatory limitations that attend the use of possibly invasive means of acquiring information. For example, the Foreign Intelligence Surveillance Act (FISA) provides fairly rigorous statutory procedures that must be honored before electronic surveillance or physical searches may be authorized in a national security context.[97] It also supplies statutory conditions under which information acquired using those techniques may be used,[98] and both judicial and legislative oversight procedures.[99] As an additional safeguard, it also calls for the creation and implementation of minimization procedures to protect private information relating to Americans consistent with the U.S. foreign intelligence interests.[100]

(...continued)

3414(a)(5)(B); 50 U.S.C. 436(a)(4).

[95] "[T]he section of the bill that previously required the Department of Justice to establish minimization procedures for National Security Letters is redrafted to reflect [the] fact that the Department adopted such procedures in October 2010," 157 *Cong. Rec*. S274 (daily ed. Jan. 26, 2011)(statement of Sen. Leahy).

[96] S. 1073, §1; S. 1050, §5; S. 1070, §5.

[97] 50 U.S.C. 1801-1829.

[98] *E.g.*, 50 U.S.C. 1806.

[99] *E.g.*, 50 U.S.C. 1805, 1808.

[100] *E.g.*, 50 U.S.C. 1802(a)(2). See 50 U.S.C. 1801(h)("'Minimization procedures', with respect to electronic surveillance, means – (1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information; (2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in subsection (e)(1) of this section, shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance; (3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes; and (4) notwithstanding paragraphs (1), (2), and (3), with respect to any electronic surveillance approved pursuant to section 1802(a) of this title, procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours unless a court order under section 1805 of this title is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person").

Section 119(f) of the USA PATRIOT Improvement and Reauthorization Act directed the Attorney General and the Director of National Intelligence to report to the congressional intelligence and judiciary committees on the feasibility of NSL minimization procedures "to ensure the protection of the constitutional rights of United States persons."[101] The Inspector General's reports noted the need for minimization standards or their regulatory equivalent:

> In our first NSL report, the OIG noted the proviso in the Attorney General's NSI Guidelines that national security investigations should use the "least intrusive collection techniques feasible" to carry out the investigations. The OIG reported that we found no clear guidance on how Special Agents should reconcile the Attorney General guidelines' limitations with the expansive authority provided in the NSL statutes. Our concerns over the lack of formal guidance were magnified because of the volume of NSLs generated by the FBI each year and because the information collected is retained for long periods in databases available to many authorized law enforcement personnel.[102]

The Justice Department convened a working group to study and make recommendations concerning possible NSL minimization standards in response to its statutory obligation and the Inspector General's initial report.[103]

Attorney General Holder reported in a letter dated December 9, 2010, to Senator Leahy as Chair of the Senate Judiciary Committee, that the Attorney General had "approved Procedures for the Collection, Use and Storage of Information Derived from National Security Letters on October 1, 2010" and that, "[t]he FBI's current practice is consistent with the procedures and the FBI is working on formal policy to implement them. In addition DOJ and ODNI [Office of the Director of National Intelligence] will shortly complete work on a joint report to Congress on NSL 'minimization' as required by the PATRIOT Reauthorization Act of 2005."[104]

The Senate Judiciary Committee report noted that, in light of the Attorney General's action, S. 193 replaced a call for the promulgation of minimization standards with a section that would direct the "Attorney General to periodically review the procedures, taking the privacy rights and civil liberties of Americans into consideration."[105] S. 1125 and H.R. 1805 adopt the same approach.[106] Senator Paul's proposals would continue to call upon the Attorney General to

---

[101] P.L. 109-177, 120 Stat. 220 (2006).

[102] *IG Report II*, at 64; see also *id.* at 68 n.41 ("In general, information related to intelligence investigations is retained in the FBI's files (either in the paper case file or in the FBI's electronic systems) for 30 years after a case is closed, and information related to criminal investigations is retained for 20 years after a case is closed. After that time, the case information is reviewed, and information that is identified for permanent retention is transferred to the National Archives and Records Administration (NARA) for storage. Any cases not meeting the criteria for permanent retention and transfer to the NARA are destroyed"); *IG Report I*, at 110 ("neither the Attorney General's NSI Guidelines nor internal FBI policies require the purging of information derived from NSLs in FBI databases, regardless of the outcome of the investigation. Thus, once information is obtained in response to a national security letter, it is indefinitely retained and retrievable by the many authorized personnel who have access to various FBI databases").

[103] *IG Report II*, at 64.

[104] Letter from Attorney General Eric H. Holder, Jr. to Senate Judiciary Committee Chairman Patrick J. Leahy (Dec. 9, 2010), available at http://judiciary.senate.gov/resources/documents/111Documents.cfm.

[105] S.Rept. 112-13, at 7 (2011).

[106] S. 1125, §12; H.R. 1805, §12, which in both instances would provide in part, "The Attorney General shall periodically review, and revise as necessary, the procedures adopted by the Attorney General on October 1, 2010 for the collection, use, and storage of information obtained in response to a national security letter. . . . In reviewing and revising the procedures . . . the Attorney General shall give due consideration to the privacy interests of individuals and the need to protect national security."

promulgate minimization standards. His proposals, however, emphasize the need for standards that address when NSL-generated information should be disposed of, for example, "including procedures to ensure that information obtained that is outside the scope of such National Security Letter or request, is returned or destroyed."[107]

Reports and Audits

Some of the NSL statutes provide for periodic reports to various congressional committees.[108] In addition, the USA PATRIOT Improvement and Reauthorization Act instructed the Attorney General to prepare, in unclassified form, an annual report to Congress on the number of NSLs issued in the previous year.[109] The same legislation directed the Inspector General of the Department of Justice to audit and report on the use of NSL authority for calendar years 2002 through 2006.[110] S. 1125 and H.R. 1805 would expand each of these requirements.[111]

Existing law requires a public report of the number of times the Justice Department has used NSL requests for information concerning Americans.[112] S. 1125 and H.R. 1805 would demand twice yearly reports to include the number of requests sought for information on those who not the subject of investigations.[113] They would also call for audits by the Justice Department's Inspector General for the years 2007 through 2013, comparable to those which the IG conducted earlier.[114]

[107] S. 1050, §5(b)(1); S. 1070, §5(b)(1); S. 1073, §1(b)(1).

[108] 18 U.S.C. 2709(e); 15 U.S.C. 1681u(h); 15 U.S.C. 1681v(f).

[109] P.L. 109-177, §118, 120 Stat. 217 (2006), 18 U.S.C. 3511 note.

[110] P.L. 109-177, §119, 120 Stat. 219 (2006).

[111] S. 1125, §8(b); H.R. 1805,§10(b), each amending, P.L. 109-177, §118(c), 18 U.S.C. 3551 note.

[112] P.L. 109-177, §118(c), 18 U.S.C. 3511 note.

[113] S. 1125, §8(a); H.R. 1805, §8(a).

[114] S. 1125, §10(b); H.R. 1805, §10(b), each amending P.L. 109-177, §119..

Text of NSL Statutes on October 25, 2001, and Now (emphasis added)

12 U.S.C. 3414(a)(5) (on October 25, 2001)

* * *

(a) ....
(5)(A) Financial institutions, and officers, employees, and agents thereof, shall comply with a request for a customer's or entity's financial records made pursuant to this subsection by the Federal Bureau of Investigation when the Director of the Federal Bureau of Investigation (or the Director's designee) certifies in writing to the financial institution that such records are sought for foreign counter intelligence purposes *and that there are specific and articulable facts giving reason to believe that the customer or entity whose records are sought is a foreign power or the agents of a foreign power as defined in section 1801 of title 50.*
(B) The Federal Bureau of Investigation may disseminate information obtained pursuant to this paragraph only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations conducted by the Federal Bureau of Investigation, and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency.
(C) On a semiannual basis the Attorney General shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate concerning all requests made pursuant to this paragraph.
(D) No financial institution, or officer, employee, or agent of such institution, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to a customer's or entity's financial records under this paragraph.

12 U.S.C. 3414(a)(5) (now)

* * *

(a) ...
(5)(A) Financial institutions, and officers, employees, and agents thereof, shall comply with a request for a customer's or entity's financial records made pursuant to this subsection by the Federal Bureau of Investigation when the Director of the Federal Bureau of Investigation (or the Director's designee *in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director*) certifies in writing to the financial institution that such records are sought for foreign counter intelligence purposes *to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.*
(B) The Federal Bureau of Investigation may disseminate information obtained pursuant to this paragraph only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations conducted by the Federal Bureau of Investigation, and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency.

(C) On the dates provided in section 415b of Title 50, the Attorney General shall fully inform the congressional intelligence committees (as defined in section 401a of Title 50) concerning all requests made pursuant to this paragraph.

(D) Prohibition of certain disclosure.—

(i) *If the Director of the Federal Bureau of Investigation, or his designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director, certifies that otherwise there may result a danger to the national security of the United States, interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person,* no financial institution, or officer, employee, or agent of such institution, shall disclose to any person *(other than those to whom such disclosure is necessary to comply with the request or an attorney to obtain legal advice or legal assistance with respect to the request)* that the Federal Bureau of Investigation has sought or obtained access to a customer's or entity's financial records under subparagraph (A).

(ii) The request shall notify the person or entity to whom the request is directed of the nondisclosure requirement under clause (i).

(iii) Any recipient disclosing to those persons necessary to comply with the request or to an attorney to obtain legal advice or legal assistance with respect to the request shall inform such persons of any applicable nondisclosure requirement. Any person who receives a disclosure under this subsection shall be subject to the same prohibitions on disclosure under clause (i).

(iv) At the request of the Director of the Federal Bureau of Investigation or the designee of the Director, any person making or intending to make a disclosure under this section shall identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request, except that nothing in this section shall require a person to inform the Director or such designee of the identity of an attorney to whom disclosure was made or will be made to obtain legal advice or legal assistance with respect to the request for financial records under subparagraph (A).

15 U.S.C. 1681u(a), (b)(on October 25, 2001)

(a) Identity of financial institutions

Notwithstanding section 1681b of this title or any other provision of this subchapter, a consumer reporting agency shall furnish to the Federal Bureau of Investigation the names and addresses of all financial institutions (as that term is defined in section 3401 of Title 12) at which a consumer maintains or has maintained an account, to the extent that information is in the files of the agency, when presented with a written request for that information, signed by the Director of the Federal Bureau of Investigation, or the Director's designee, which certifies compliance with this section. The Director or the Director's designee may make such a certification only if the Director or the Director's designee has determined in writing that—

(1)such information is necessary for the conduct of an authorized foreign counterintelligence investigation; and

(2) there are specific and articulable facts giving reason to believe that the consumer—

(A) is a foreign power (as defined in section 1801 of title 50) or a person who is not a United States person (as defined in such section 1801 of title 50) and is an official of a foreign power; or

(B) is an agent of a foreign power and is engaging or has engaged in an act of international terrorism (as that term is defined in section 1801(c) of title 50) or clandestine intelligence activities that involve or may involve a violation of criminal statutes of the United States.

(b) Identifying information

Notwithstanding the provisions of section 1681b of this title or any other provision of this subchapter, a consumer reporting agency shall furnish identifying information respecting a consumer, limited to name, address, former addresses, places of employment, or former places of employment, to the Federal Bureau of Investigation when presented with a written request, signed by the Director or the Director's designee, which certifies compliance with this subsection. The Director or the Director's designee may make such a certification only if the Director or the Director's designee has determined in writing that—

(1) such information is necessary to the conduct of an authorized counterintelligence investigation; and

(2) there is information giving reason to believe that the consumer has been, or is about to be, in contact with a foreign power or an agent of a foreign power (as defined in section 1801 of title 50).

* * *

15 U.S.C. 1681u(a), (b)(now)

(a) Identity of financial institutions

Notwithstanding section 1681b of this title or any other provision of this subchapter, a consumer reporting agency shall furnish to the Federal Bureau of Investigation the names and addresses of all financial institutions (as that term is defined in section 3401 of Title 12) at which a consumer maintains or has maintained an account, to the extent that information is in the files of the agency, when presented with a written request for that information, signed by the Director of the Federal Bureau of Investigation, or the Director's designee *in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge of a Bureau field office designated by the Director*, which certifies compliance with this section. The Director or the Director's designee may make such a certification only if the Director or the Director's designee has determined in writing, that *such information is sought for the conduct of an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.*

(b) Identifying information

Notwithstanding the provisions of section 1681b of this title or any other provision of this subchapter, a consumer reporting agency shall furnish identifying information respecting a consumer, limited to name, address, former addresses, places of employment, or former places of employment, to the Federal Bureau of Investigation when presented with a written request, signed by the Director or the Director's designee *in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge of a Bureau field office designated by the Director*, which certifies compliance with this subsection. The Director or the Director's designee may make such a certification only if the Director or the Director's designee has determined in writing that *such information is sought for the conduct of an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an*

investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

* * *

18 U.S.C. 2709 (as of October 25, 2001)

(a) Duty to provide.—A wire or electronic communication service provider shall comply with a request for subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession made by the Director of the Federal Bureau of Investigation under subsection (b) of this section.
(b) Required certification.—The Director of the Federal Bureau of Investigation, or his designee in a position not lower than Deputy Assistant Director, may—
(1) request the name, address, length of service, and local and long distance toll billing records of a person or entity if the Director (or his designee in a position not lower than Deputy Assistant Director) certifies in writing to the wire or electronic communication service provider to which the request is made that—

(A) the name, address, length of service, and toll billing records sought are relevant to an authorized investigation to foreign counterintelligence investigation; and
(*B) there are specific and facts giving reason to believe that the person or entity to whom the information sought pertains is a foreign power or an agent of a foreign power as defined in section 101 of the Foreign intelligence Surveillance Act of 1978 (50 U.S.C. 1801*); and

(2) request the name, address, and length of service of a person or entity if the Director (or his designee in a position not lower than Deputy Assistant Director) certifies in writing to the wire or electronic communication service provider to which the request is made that—

(A) the information sought is relevant to an authorized foreign counterintelligence investigation; and
(B) There are specific and articulable facts giving reason to believe that communication facilities registered in the name of the person or entity have been used, through the services of such provider, in communications with—

(i) an individual who is engaging or has engaged in international terrorism as defined in section 101(c) of the Foreign Intelligence Surveillance Act or clandestine intelligence activities that involve or may involve a violation of the criminal statutes of the United States; or
(ii)a foreign power or agent of a foreign power under circumstances giving reason to believe that the communication concerned international terrorism as defined in section 101(c) of the Foreign Intelligence Surveillance Act or clandestine intelligence activities that involve or may involve a violation of the criminal statutes of the United States.

(c) Prohibition of certain disclosure.—No wire or electronic communication service provider, or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.
(d) Dissemination by bureau.—The Federal Bureau of Investigation may disseminate information and records obtained under this section only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations conducted by the Federal Bureau of Investigation, and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency.

(e) Requirement that certain congressional bodies be informed.—On a semiannual basis the Director of the Federal Bureau of Investigation shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate, and the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate, concerning all requests made under subsection (b) of this section.

18 U.S.C. 2709 (now)

(a) Duty to provide.—A wire or electronic communication service provider shall comply with a request for subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession made by the Director of the Federal Bureau of Investigation under subsection (b) of this section.
(b) Required certification.—The Director of the Federal Bureau of Investigation, or his designee in a position not lower than Deputy Assistant Director *at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director*, may—

(1) request the name, address, length of service, and local and long distance toll billing records of a person or entity if the Director (or his designee) certifies in writing to the wire or electronic communication service provider to which the request is made that the name, address, length of service, and toll billing records *sought are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States.*; and

(2) request the name, address, and length of service of a person or entity if the Director (or his designee) certifies in writing to the wire or electronic communication service provider to which the request is made that the information *sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States*.

(c) Prohibition of certain disclosure.—
(1) *If the Director of the Federal Bureau of Investigation, or his designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director, certifies that otherwise there may result a danger to the national security of the United States, interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person,* no wire or electronic communications service provider, or officer, employee, or agent thereof, shall disclose to any person (other than those to whom such disclosure is necessary to comply with the request or an attorney to obtain legal advice or legal assistance with respect to the request) that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.
(2) The request shall notify the person or entity to whom the request is directed of the nondisclosure requirement under paragraph (1).
(3) Any recipient disclosing to those persons necessary to comply with the request or to an attorney to obtain legal advice or legal assistance with respect to the request shall inform such person of any applicable nondisclosure requirement. Any person who receives a disclosure under this subsection shall be subject to the same prohibitions on disclosure under paragraph (1).

(4) At the request of the Director of the Federal Bureau of Investigation or the designee of the Director, any person making or intending to make a disclosure under this section shall identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request, except that nothing in this section shall require a person to inform the Director or such designee of the identity of an attorney to whom disclosure was made or will be made to obtain legal advice or legal assistance with respect to the request under subsection (a).
(d) Dissemination by bureau.—The Federal Bureau of Investigation may disseminate information and records obtained under this section only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations conducted by the Federal Bureau of Investigation, and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency.
(e) Requirement that certain congressional bodies be informed.—On a semiannual basis the Director of the Federal Bureau of Investigation shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate, and the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate, concerning all requests made under subsection (b) of this section.
(f) Libraries.—A library (as that term is defined in section 213(1) of the Library Services and Technology Act (20 U.S.C. 9122(1)), the services of which include access to the Internet, books, journals, magazines, newspapers, or other similar forms of communication in print or digitally by patrons for their use, review, examination, or circulation, is not a wire or electronic communication service provider for purposes of this section, unless the library is providing the services defined in section 2510(15) ("electronic communication service") of this title.

15 U.S.C. 1681v (as of October 25, 2001)

NONE. This section was created by the USA PATRIOT Act, effective October 26, 2001.

15 U.S.C. 1681v (now)

(a) Disclosure
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.

(b) Form of certification
The certification described in subsection (a) of this section shall be signed by a supervisory official designated by the head of a Federal agency or an officer of a Federal agency whose appointment to office is required to be made by the President, by and with the advice and consent of the Senate.

(c) Confidentiality
(1) If the head of a government agency authorized to conduct investigations of intelligence or counterintelligence activities or analysis related to international terrorism, or his designee, certifies that otherwise there may result a danger to the national security of the United States, interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person, no consumer reporting agency or officer, employee, or agent of such consumer reporting agency, shall disclose to any person (other than those to whom such disclosure is necessary to comply with the request or an attorney to obtain legal advice or legal assistance with respect to the request), or specify in any consumer report, that a government agency has sought or obtained access to information under subsection (a) of this section.
(2) The request shall notify the person or entity to whom the request is directed of the nondisclosure requirement under paragraph (1).
(3) Any recipient disclosing to those persons necessary to comply with the request or to any attorney to obtain legal advice or legal assistance with respect to the request shall inform such persons of any applicable nondisclosure requirement. Any person who receives a disclosure under this subsection shall be subject to the same prohibitions on disclosure under paragraph (1).
(4) At the request of the authorized government agency, any person making or intending to make a disclosure under this section shall identify to the requesting official of the authorized government agency the person to whom such disclosure will be made or to whom such disclosure was made prior to the request, except that nothing in this section shall require a person to inform the requesting official of the identity of an attorney to whom disclosure was made or will be made to obtain legal advice or legal assistance with respect to the request for information under subsection (a) of this section.

(d) Rule of construction
Nothing in section 1681u of this title shall be construed to limit the authority of the Director of the Federal Bureau of Investigation under this section.

(e) Safe harbor
Notwithstanding any other provision of this subchapter, any consumer reporting agency or agent or employee thereof making disclosure of consumer reports or other information pursuant to this section in good-faith reliance upon a certification of a government agency pursuant to the provisions of this section shall not be liable to any person for such disclosure under this subchapter, the constitution of any State, or any law or regulation of any State or any political subdivision of any State.

(f) Reports to Congress
(1) On a semi-annual basis, the Attorney General shall fully inform the Committee on the Judiciary, the Committee on Financial Services, and the Permanent Select Committee on Intelligence of the House of Representatives and the Committee on the Judiciary, the Committee on Banking, Housing, and Urban Affairs, and the Select Committee on Intelligence of the Senate concerning all requests made pursuant to subsection (a) of this section.
(2) In the case of the semiannual reports required to be submitted under paragraph (1) to the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate, the submittal dates for such reports shall be as provided in section 415b of Title 50.

50 U.S.C. 436 (as of October 25, 2001)

(a) Generally

(1) Any authorized investigative agency may request from any financial agency, financial institution, or holding company, or from any consumer reporting agency, such financial records, other financial information, and consumer reports as may be necessary in order to conduct any authorized law enforcement investigation, counterintelligence inquiry, or security determination. Any authorized investigative agency may also request records maintained by any commercial entity within the United States pertaining to travel by an employee in the executive branch of Government outside the United States.

(2) Requests may be made under this section where—

(A) the records sought pertain to a person who is or was an employee in the executive branch of Government required by the President in an Executive order or regulation, as a condition of access to classified information, to provide consent, during a background investigation and for such time as access to the information is maintained, and for a period of not more than three years thereafter, permitting access to financial records, other financial information, consumer reports, and travel records; and

(B)(i) there are reasonable grounds to believe, based on credible information, that the person is, or may be, disclosing classified information in an unauthorized manner to a foreign power or agent of a foreign power;

(ii) information the employing agency deems credible indicates the person has incurred excessive indebtedness or has acquired a level of affluence which cannot be explained by other information known to the agency; or

(iii) circumstances indicate the person had the capability and opportunity to disclose classified information which is known to have been lost or compromised to a foreign power or an agent of a foreign power.

(3) Each such request—

(A) shall be accompanied by a written certification signed by the department or agency head or deputy department or agency head concerned, or by a senior official designated for this purpose by the department or agency head concerned (whose rank shall be no lower than Assistant Secretary or Assistant Director), and shall certify that—

(i) the person concerned is or was an employee within the meaning of paragraph (2)(A);

(ii) the request is being made pursuant to an authorized inquiry or investigation and is authorized under this section; and

(iii) the records or information to be reviewed are records or information which the employee has previously agreed to make available to the authorized investigative agency for review;

(B) shall contain a copy of the agreement referred to in subparagraph (A)(iii);

(C) shall identify specifically or by category the records or information to be reviewed; and

(D) shall inform the recipient of the request of the prohibition described in subsection (b) of this section.

(b) *Disclosure of requests*

Notwithstanding any other provision of law, no governmental or private entity, or officer, employee, or agent of such entity, may disclose to any person that such entity has received or satisfied a request made by an authorized investigative agency under this section.

* * *

50 U.S.C. 436 (now)

(a) Generally
(1) Any authorized investigative agency may request from any financial agency, financial institution, or holding company, or from any consumer reporting agency, such financial records, other financial information, and consumer reports as may be necessary in order to conduct any authorized law enforcement investigation, counterintelligence inquiry, or security determination. Any authorized investigative agency may also request records maintained by any commercial entity within the United States pertaining to travel by an employee in the executive branch of Government outside the United States.

(2) Requests may be made under this section where—
(A) the records sought pertain to a person who is or was an employee in the executive branch of Government required by the President in an Executive order or regulation, as a condition of access to classified information, to provide consent, during a background investigation and for such time as access to the information is maintained, and for a period of not more than three years thereafter, permitting access to financial records, other financial information, consumer reports, and travel records; and
(B)(i) there are reasonable grounds to believe, based on credible information, that the person is, or may be, disclosing classified information in an unauthorized manner to a foreign power or agent of a foreign power;
(ii) information the employing agency deems credible indicates the person has incurred excessive indebtedness or has acquired a level of affluence which cannot be explained by other information known to the agency; or
(iii) circumstances indicate the person had the capability and opportunity to disclose classified information which is known to have been lost or compromised to a foreign power or an agent of a foreign power.
(3) Each such request—
(A) shall be accompanied by a written certification signed by the department or agency head or deputy department or agency head concerned, or by a senior official designated for this purpose by the department or agency head concerned (whose rank shall be no lower than Assistant Secretary or Assistant Director), and shall certify that—
(i) the person concerned is or was an employee within the meaning of paragraph (2)(A);
(ii) the request is being made pursuant to an authorized inquiry or investigation and is authorized under this section; and
(iii) the records or information to be reviewed are records or information which the employee has previously agreed to make available to the authorized investigative agency for review;
(B) shall contain a copy of the agreement referred to in subparagraph (A)(iii);
(C) shall identify specifically or by category the records or information to be reviewed; and
(D) shall inform the recipient of the request of the prohibition described in subsection (b) of this section.

(b) *Prohibition of certain disclosure*
(1) *If an authorized investigative agency described in subsection (a) of this section certifies that otherwise there may result a danger to the national security of the United States, interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person,* no governmental or private entity, or officer, employee, or agent of such entity, may disclose to any person *(other than those to*

whom such disclosure is necessary to comply with the request or an attorney to obtain legal advice or legal assistance with respect to the request) that such entity has received or satisfied a request made by an authorized investigative agency under this section.

(2) The request shall notify the person or entity to whom the request is directed of the nondisclosure requirement under paragraph (1).

(3) Any recipient disclosing to those persons necessary to comply with the request or to an attorney to obtain legal advice or legal assistance with respect to the request shall inform such persons of any applicable nondisclosure requirement. Any person who receives a disclosure under this subsection shall be subject to the same prohibitions on disclosure under paragraph (1).

(4) At the request of the authorized investigative agency, any person making or intending to make a disclosure under this section shall identify to the requesting official of the authorized investigative agency the person to whom such disclosure will be made or to whom such disclosure was made prior to the request, except that nothing in this section shall require a person to inform the requesting official of the identity of an attorney to whom disclosure was made or will be made to obtain legal advice or legal assistance with respect to the request under subsection (a) of this section.

* * *

Author Contact Information

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