Statement of David Kris
before the
Subcommittee on the Constitution, Civil Rights and Civil Liberties
of the House Committee on the Judiciary
Hearing on H.R. 3189, the National Security Letters Reform Act of 2007
April 15, 2008

Chairman Nadler and Ranking Member Franks, thank you for the opportunity to testify concerning national security letters (NSLs).[1] I support legislation that would replace the various NSL statutes currently used by the FBI and other federal agencies in conducting national security investigations and related activities.[2] I believe that Chairman Nadler's bill, H.R. 3189, is an excellent vehicle for further discussion leading to reform in this important area, and I have submitted comments on it to the staff.

But I would go further. I believe Congress should enact a single statute, providing for national security subpoenas, to replace all of the current NSL provisions. This would streamline and simplify current law, which is both intricate and idiosyncratic, as shown in the summary table at Tab 1. A single statute would also allow a considered, global resolution of the difficult policy questions that necessarily attend the use of any national security subpoena power.

I believe a new national security subpoena statute should contain or satisfy 10 essential elements, which are listed, and then discussed, beginning on the next page. For illustrative purposes, to present my views in more concrete terms, I have drafted a statute that reflects those 10 elements. It appears at Tab 2.[3]

Again, I appreciate your invitation to testify, and I look forward to answering any questions the Subcommittee may have. Thank you.

* * *

[1] I am testifying solely in my individual capacity, not as a representative of any former or current employer. This testimony was cleared for publication under 28 C.F.R. § 17.18.

[2] See 12 U.S.C. § 3414 (RFPA); 15 U.S.C. § 1681u (FCRAu); 15 U.S.C. § 1681v (FCRAv); 18 U.S.C. § 2709 (ECPA); 50 U.S.C. § 436 (National Security Act); cf. 50 U.S.C. § 1861 (Patriot Act Section 215).

[3] I am sure that my proposed statute could be improved or replaced by a competent drafter; I am submitting it only to illustrate the discussion in concrete terms. More generally, I stress the tentative nature of my testimony, which is in part the product of a relatively brief period of thought unaided by inside knowledge of the current operational and threat environment (I was first contacted about the possibility of testifying one week ago). My primary purpose here is to raise issues and provide technical support, not to take a strong position on any particular question.

I believe Congress should enact a single statute, providing for national security subpoenas, to replace all of the current NSL provisions. This subpoena statute should contain or satisfy the following 10 elements. It should:

(1) streamline and simplify current law, which is unnecessarily and harmfully complex;

(2) provide for subpoenas to be issued by attorneys designated by the Attorney General;

(3) make subpoenas available to all Intelligence Community agencies, as long as the subpoena is issued by a designated attorney for the government as described in (2) above, and limited to obtaining the types of information described in (5) below, and also subject, as desired, to additional limits for particular agencies (*e.g.*, CIA);

(4) allow production of any tangible thing that is subject to compelled production via grand jury subpoena;

(5) be limited to acquiring certain specified foreign intelligence information and Secret Service protective information, subject to additional limits by analogy to 50 U.S.C. § 1861(b)(2)(A) if desired;

(6) impose a nondisclosure obligation on recipients, with the usual exceptions, that expires 60 days after a written objection is received by the government, unless the government obtains an extension order from the Foreign Intelligence Surveillance Court (FISC) – an approach that should satisfy *Doe v. Gonzales*, 500 F. Supp. 2d 379 (SDNY 2007);

(7) permit motions to quash, and to enforce, subpoenas in the FISC, using the "burdensome or oppressive" standard applicable to grand jury subpoenas under Fed. R. Crim. P. 17(c) and *United States v. R. Enterprises, Inc.*, 498 U.S. 292 (1991);

(8) provide the usual sort of prospective immunity for good-faith compliance;

(9) require minimization procedures governing acquisition, retention and dissemination of information, and limits on the use of that information, along the lines of current 50 U.S.C. § 1861(g); and

(10) adhere to the traditional oversight standard in requiring (and enabling) the Attorney General to keep the Congressional Intelligence and Judiciary Committees, as well as certain other Committees, "fully informed" on a semi-annual basis, and provide for three successive annual audits by the Justice Department's Inspector General.

As noted above, a proposed statute reflecting these elements is set forth at Tab 2. Beginning on the next page, I discuss each element in more detail, and in concrete terms, by reference to the language used in the proposed statute, subject to the caveats in footnote 3 above.

* * *

1. Streamline and Simplify Current Law.

Today, there are five NSL statutes, that impose various substantive and procedural requirements, on various federal agencies, conducting various investigations or activities, seeking various kinds of information, from various types of third parties.[4] There are also other collection statutes, with their own varying standards, that overlap to some degree with the NSL statutes.[5] Some of these variations make sense, but some do not. Two recent reports from the Department of Justice's Inspector General (IG) describe the cost of such variation.[6] To cite one example, the IG reports show that FBI agents do not always appreciate the difference between a FCRAu NSL and a FCRAv NSL.[7] This means that they are sometimes slow to use these authorities, and sometimes use them incorrectly – in other words, that national security and civil liberties both suffer. The FBI itself is not primarily to blame for this; the current statutory regime is Byzantine. The intricacy results from an iterative, evolutionary legislative process, conducted over a period of many years, punctuated by September 11. Where evolution has produced such a messy result, however, Congress should impose an intelligent design.

2. Subpoenas Issued by Designated Attorneys.

The proposed statute at Tab 2 provides for national security subpoenas to replace the current regime of national security letters. These national security subpoenas would be issued by the Attorney General or a designated attorney for the government – in most cases, a Justice Department lawyer, whether at Main Justice or a U.S. Attorney's Office.[8] By requiring the involvement of DOJ attorneys, the statute mirrors practice involving grand jury subpoenas and many administrative subpoenas, and splits the difference between national security letters, which are issued by FBI agents, and Patriot Act Section 215 orders,[9] which are issued by judges. According to the recent IG reports, FBI agents have misused national security letters, and require additional oversight. In the current environment, however, Section 215's requirement for advance judicial approval seems too cumbersome for the large number of NSLs that are issued each year (nearly 50,000 issued by the FBI alone in 2006).[10]

---

[4] 12 U.S.C. § 3414 (RFPA); 15 U.S.C. § 1681u (FCRAu); 15 U.S.C. § 1681v (FCRAv); 18 U.S.C. § 2709 (ECPA); 50 U.S.C. § 436 (National Security Act).

[5] See, *e.g.*, 50 U.S.C. § 1861 (Patriot Act Section 215).

[6] See http://www.usdoj.gov/oig/special/s0803b/final.pdf (hereinafter 2008 IG NSL Report); http://www.usdoj.gov/oig/special/s0703b/final.pdf (hereinafter 2007 IG NSL Report).

[7] See 2008 IG NSL Report at 89.

[8] Under Fed. R. Crim. P. 1(b), an "attorney for the government" is defined to be: "(A) the Attorney General or an authorized assistant; (B) a United States attorney or an authorized assistant; (C) when applicable to cases arising under Guam law, the Guam Attorney General or other person whom Guam law authorizes to act in the matter; and (D) any other attorney authorized by law to conduct proceedings under these rules as a prosecutor." This would include, for example, National Security Division attorneys at Main Justice, and AUSAs in the field. Cf. *United States v. Sells Engineering, Inc.*, 463 U.S. 418, 426 & n.8 (1983).

[9] 50 U.S.C. § 1861.

[10] See 2008 IG NSL Report at 9.

There will be strong opposition to the idea that designated attorneys, rather than FBI agents or other personnel, issue the subpoenas. This opposition probably will be expressed in terms of speed and agility – *e.g.*, that Assistant U.S. Attorneys and Main Justice lawyers may be unavailable at certain times, especially in rural areas; or that even if they are available, it will take too long to contact them. This objection, however, is hard to square with (1) the extensive process already required by the FBI before an NSL may be issued, as described in the two IG reports and in comprehensive guidance issued by the FBI in 2007;[11] and (2) the fact that, in most field offices, there is only one person – the SAC – who may authorize an NSL (in the NY, DC, and LA field offices, the FBI Assistant Directors may also do so; at FBI Headquarters, a handful of other officials may do so).[12] Replacing these officials with five or more designated AUSAs in small districts, and 10 or more designated AUSAs in larger districts, as well as a reasonable number of attorneys in the National Security Division at Main Justice, would significantly expand the pool of eligible officials, and almost surely speed up the process.

3. Subpoenas Available to All Intelligence Community Agencies.

The proposed statute applies not only to the FBI, but also to any other member of the Intelligence Community that may conduct investigations or other activities (*e.g.*, analysis) under Executive Order 12333, and to the Secret Service in performing its protective functions. I recognize that the final version of any national security subpoena statute may limit the subpoena power of certain Intelligence Community agencies, such as the CIA. Those limits, however, will need to be determined by a process that requires more time and consultation than is available to me now.

Under current law, as shown in the summary table at Tab 1, two NSL statutes (FCRAu and ECPA) apply only to the FBI, while three statutes (FCRAv, the National Security Act, and RFPA) apply to the FBI and to other agencies. In particular, of those three broader statutes, FCRAv applies to any government agency authorized to conduct investigations or other intelligence activities related to international terrorism; the National Security Act applies primarily to any authorized investigative agency conducting investigations of executive branch employees with security clearances (*e.g.*, espionage investigations); and RFPA applies to any governmental authority conducting any foreign counterintelligence or affirmative intelligence activity, and to the Secret Service in performing its protective functions.

Ultimately, these restrictions depend in large part on Executive Order 12333, because – at least in the absence of statutory charters for the Intelligence Community – it prescribes the types of investigations, and investigative methods, available to each member of the Community. The proposed statute expressly refers to the executive order in an effort to simplify current law, and

---

[11] The FBI guidance is available at http://epic.org/privacy/nsl/New_NSL_Guidelines.pdf.

[12] Currently, FBI lawyers known as Chief Division Counsels (CDCs) review all NSL requests, but the recent IG reports have cast doubt on the independence of their review, in light of their reporting structure. See 2007 IG NSL Report at xliii ("We found that … some [CDCs] have been reluctant to question the predication for NSL requests or the relevance of the information sought"); 2008 IG NSL Report at 45.

to make explicit what is now implicit – i.e., that the President determines which agencies may use NSL statutes by determining which may conduct investigations or analysis related to international terrorism or other subjects specified in the current NSL statutes.

The one notable exception to the primacy of Executive Order 12333 in this area is the law enforcement proviso of the National Security Act of 1947, which provides that the CIA "shall have no police, subpoena, or law enforcement powers or internal security functions."[13] Currently, RFPA, FCRAv, and the National Security Act NSL provisions are exceptions to that general proviso for certain types of information sought in certain types of investigations. In its current baseline form, the proposed statute would eliminate these restrictions and treat the CIA like any other Intelligence Community member, subject to the limits in Executive Order 12333 – and subject to the essential requirements that the subpoena be issued by an attorney for the government designated by the Attorney General (as discussed in part 2, above), and that it seek only the kinds of information specified in the statute (as discussed in part 5, below). Even today, the CIA may engage in the "collection of foreign intelligence or counterintelligence within the United States," as long as such collection is "coordinated with the FBI as required by procedures agreed upon by the Director of Central Intelligence and the Attorney General."[14]

Recognition that CIA and DOD may issue NSLs under current law has generated controversy.[15] Granting these agencies even broader subpoena authority may be a bridge too far. If desired, CIA's (or any agency's) use of national security subpoenas could be limited or forbidden by adding appropriate language to subsection (a)(1) of the proposed statute. As a technical matter, this would not be hard to do once the substance of the limits is determined. I have not attempted it here, however, primarily because such determination may require extended consideration and consultation between the Legislative and Executive Branches. All I can do for now is flag the issue for later resolution, without taking a position.

4. Subpoenas Available for All Tangible Things Subject to Grand Jury Subpoena.

The proposed statute applies to "any tangible thing (including books, records, papers, documents, and other items)," and is meant to reach broadly, subject to the specific limits described below. For example, the word "tangible" is meant to include not only physical objects, such as a paper billing records, but also electronic records; the word is used here in much the same way as it is used in copyright law.[16]

[13] 50 U.S.C. § 403-4a(d)(1).

[14] Executive Order 12333 § 1.8(a). Since the executive order was issued, of course, the Director of Central Intelligence has been replaced by the Director of National Intelligence, who is not the Director of the CIA.

[15] See, *e.g.*, http://www.nytimes.com/2007/01/14/washington/14spy.html?_r=1&oref=slogin.

[16] See 17 U.S.C. § 102 (referring to work "fixed in any tangible medium of expression, now known or later developed, from which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device").

Although it extends to electronic data, the proposed statute would not replace FISA's current provisions authorizing surveillance using pen registers and trap and trace devices.[17] That is primarily because pen-trap surveillance collects information that is not yet in existence at the time of the court order – i.e., it imposes a continuing obligation to produce the information over a period of time – while an NSL is generally thought only to require production of information already in existence at the time it is issued. As telecommunications providers increasingly create and maintain real-time electronic billing records, of course, a series of NSLs could effectively mimic pen-trap surveillance. It therefore may make sense to reconsider the legal distinctions between them; it would be possible, for example, to modify the subpoena statute expressly to include pen-trap surveillance.

The proposed statute does not distinguish between various kinds of tangible things, as long as they are subject to production via grand jury subpoena. Thus, for example, a national security subpoena could be used to obtain information and records not subject to any of the current NSL statutes, including those from state motor vehicle agencies, hotels, landlords, storage facilities, and other entities.[18] A report by the DOJ Inspector General reveals that from 2002 to 2006, the FBI requested 16 different types of records using Patriot Act Section 215 orders, which generally are used only when NSLs are not available.[19] If desired, of course, a subset of tangible things could be carved out of the national security subpoena statute, and remain available only via court order under Patriot Act Section 215, or subject to some other substantive or procedural limit.[20]

The proposed statute begins with the phrase, "Notwithstanding any other law," primarily to eliminate uncertainty about the effect of federal or state laws that condition the disclosure of certain information via grand jury subpoena. For example, the Buckley Amendment permits disclosure of educational records "pursuant to any lawfully issued subpoena," but requires notice to the student and parents prior to such disclosure.[21] According to the recent IG report, DOJ at one point concluded that notice would likewise be required under Section 215 of the Patriot Act, because Section 215 did not purport to apply "Notwithstanding any other law."[22] The proposed

---

[17] 50 U.S.C. §§ 1841-1846.

[18] The original version of FISA's business records provision, before it was amended by Section 215 of the Patriot Act, applied to transportation common carriers, physical storage facilities, public accommodation facilities, and vehicle rental facilities. 50 U.S.C. §§ 1861-1862 (prior to Patriot Act amendment). The legislative history explains that these four categories were included in the original statute "because of their frequent use by subjects of FBI foreign intelligence and international terrorism investigations." S. Rep. No. 185, 105th Cong. 2d Sess. 29 (1998).

[19] See http://www.usdoj.gov/oig/special/s0803a/final.pdf (hereinafter 2008 IG 215 Report) at 19.

[20] See, *e.g.*, 50 U.S.C. § 1861(a)(3) (referring to "library circulation records, library patron lists, book sales records, book customer lists, firearms sales records, tax return records, educational records, or medical records containing information that would identify a person").

[21] 20 U.S.C. § 1232g.

[22] See http://www.usdoj.gov/oig/special/s0703a/final.pdf (hereinafter 2007 IG 215 Report) at x, xvi.

statute includes that phrase to make clear that notice would not be required, despite the Buckley Amendment or other such laws.[23]

5. Subpoenas Limited to Certain Foreign Intelligence and Protective Information.

The proposed statute applies where the tangible things sought by the subpoena constitute or contain any of the following three kinds of information:

> (1) information that relates to the ability of the United States to protect against actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power, sabotage or international terrorism by a foreign power or an agent of a foreign power; or clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power;[24]
>
> (2) information with respect to a foreign power or foreign territory that relates to the national defense or the security of the United States, or the conduct of the foreign affairs of the United States, but does not concern a United States person;[25] or
>
> (3) information relevant to the protective functions of the Secret Service as described in 18 U.S.C. §§ 3056 and 3056A, which authorize protection of the President and the Vice President (and their immediate families), visiting foreign heads of state and other distinguished foreign visitors, and certain other persons.

This standard is both somewhat narrower and somewhat broader than current law. It is narrower than current law because, with respect to information concerning U.S. persons, it requires a direct link to the protective goals set forth in the statute. Current law, by contrast, requires only that information be relevant to, or sought for, an authorized *investigation*, the precise operational scope of which is determined by the government.[26] Thus, as the FBI has advised its agents, current law is satisfied by "a reasonable belief that the information sought via the NSL either supports or weakens facts being investigated in a case."[27] Requiring a direct link between the information sought and the statutorily defined protective purposes – unmediated by the more nebulous contours of the investigation – should prevent misuse of subpoenas even if, in any given case, an investigation has improperly expanded. This may be particularly useful in curbing any real or imagined "community of interest" abuses, whereby NSLs might be used to obtain records pertaining to persons several degrees of separation removed from the subject of an investigation.

---

[23] There is a possible anomaly, involving 18 U.S.C. §§ 2703(a) and (b)(1)(B)(i), that may need to be addressed here.

[24] Cf. 50 U.S.C. § 1801(e)(1).

[25] Cf. 50 U.S.C. § 1801(e)(2). It would also be possible to expand this second category to include information concerning a U.S. person. That might require consultations between the Legislative and Executive Branches.

[26] See, *e.g.*, 15 U.S.C. § 1681u(a)-(b).

[27] See http://epic.org/privacy/nsl/New_NSL_Guidelines.pdf at 5.

If further narrowing is desired, a variation on the standard in Patriot Act Section 215 could be considered. Under that provision, tangible things are presumed to be "relevant" to an authorized investigation, and therefore subject to production via FISA Court order, if they "pertain to" any of the following: (i) a foreign power or agent of a foreign power; (ii) the activities of a "suspected" agent of a foreign power who is the subject of an authorized investigation; or (iii) an individual who is "in contact with, or known to," such a suspected agent of a foreign power.[28] Expressed in reverse – as a rebuttable presumption *against* relevance in the *absence* of one of the three scenarios – such a provision would limit possible abuses, but might still be tolerable to the government, particularly because the presumption could be rebutted as needed in particular cases.[29] On the other hand, there is some indication, in the partially redacted portions of the recent IG report on Section 215, that this provision may have led to some confusion and difficulty, in which case further discussions with the government might be required before adopting the language.[30]

In any event, the standard in the proposed subpoena statute at Tab 2 is also somewhat broader than current law because it refers not only to protection against international terrorism and clandestine intelligence activities, but also to protection against attack, sabotage, and other grave hostile acts committed by foreign powers or their agents. There is no reason to exclude the latter group of threats from the allowable purposes served by a subpoena. On the contrary, it is clearly sensible to incorporate as much as possible the existing and familiar definition of "foreign intelligence information" in 50 U.S.C. § 1801(e), which includes both groups of foreign threats to the national security.

6. Nondisclosure.

The proposed statute requires nondisclosure, subject to the usual exceptions, if a designated official makes a written finding concerning the usual enumerated harms. Persons subject to a nondisclosure obligation may at any time challenge the scope and duration of the obligation by filing a petition in the FISC. Alternatively, they may simply object to the nondisclosure obligation in writing – *e.g.*, by sending an e-mail or letter to the attorney for the government who issued the subpoena. Sixty days later, the nondisclosure obligation automatically expires unless the government has obtained a contrary order from the FISC. This approach is designed to comply with the decision in *Doe v. Gonzales*[31]; if the *Doe* decision is overturned in the Second Circuit, reversion to the procedures outlined in 18 U.S.C. § 3511 may be possible, if desired. Given the volume of national security letters – 50,000 per year – a requirement that the government seek court approval for nondisclosure in every case seems impractical; given the First Amendment requirements outlined in *Doe*, however, only a court may impose a long-term nondisclosure order. Requiring the subject of a nondisclosure obligation to object in writing before the government assumes the burden of going to court seems

[28] 50 U.S.C. § 1861(b)(2)(A)(i)-(iii).

[29] See generally Kris and Wilson, *National Security Investigations and Prosecutions* at 18-14 to 18-16 (West 2007).

[30] See 2008 IG 215 Report at 30.

[31] 500 F. Supp. 2d 379 (SDNY 2007).

tolerable under *Doe*, and will as a practical matter limit the number of cases in which a judicial order becomes necessary (because most persons subject to a nondisclosure obligation will not object). It does mean that a nondisclosure obligation may remain in effect without judicial review, but only where no person has lodged an objection. Of course, the Office of Legal Counsel and other First Amendment specialists should review this provision before it is enacted.

7. Judicial Review and Enforcement.

The proposed statute also permits motions to quash, and to enforce, subpoenas in the FISC, under the "burdensome or oppressive" standard applicable to grand jury subpoenas.[32]

8. Immunity.

The proposed statute contains a standard immunity provision for good-faith compliance.

9. Minimization and Use.

The proposed statute requires minimization procedures governing acquisition, retention and dissemination of information obtained from a subpoena, and limits the use of that information. Currently, Section 215 of the Patriot Act requires minimization procedures governing retention and dissemination of information, but not acquisition.[33] Conceptually, this is understandable, because a third party, rather than the government itself, collects information pursuant to a Section 215 order; the same is true of a subpoena. But I believe it makes sense for the Attorney General to establish procedures governing the scope of requests made by national security subpoena, so that they are narrowly tailored; such procedures are most conveniently cast as minimization procedures governing acquisition.[34]

10. Oversight.

The proposed statute follows the traditional oversight standard in requiring the government to keep the Congressional Intelligence and Judiciary Committees "fully informed" on a semi-annual basis; with respect to certain categories of information (*e.g.*, credit reports), other Committees of Congress are also to be kept fully informed (*e.g.*, the Senate Banking Committee). To assist the Attorney General in fulfilling these requirements, the statute allows him to require any other officer to provide information as may be necessary.[35] The statute also provides for three annual audits by the Justice Department's Inspector General.

* * *

[32] See Fed. R. Crim. P. 17(c); *United States v. R. Enterprises, Inc.*, 498 U.S. 292 (1991).

[33] 50 U.S.C. § 1861(g). I note that under USSID 18, the normal retention period for NSA raw SIGINT is five years.

[34] See Executive Order 12333 § 2.4 ("Agencies within the Intelligence Community shall use the least intrusive collection techniques feasible within the United States or directed against United States persons abroad").

[35] Cf. 50 U.S.C. §§ 1804(c)-(d).

Tab 1: Summary Table Comparing Current National Security Letter (NSL) Statutes

Authority	Who May Request Production?	From Whom?	Production of What?	Requirements	Dissemination	Oversight	Other
12 USC 3414 (RFPA)	Government authority authorized to conduct "foreign counter- or foreign positive-intelligence activities" [(a)(1)(A)], or "investigations of, or intelligence or counterintelligence analyses related to, international terrorism" [(a)(1)(C)]. The Secret Service [(a)(1)(B)]. The FBI. Recipient "shall comply"[1] with request from FBI[2] [(a)(5)(A)].	Requests may be made to a "financial institution" [see (a)(2)]. Financial institutions and various listed personnel "shall comply" with FBI request[2] [(a)(5)(A)]. Note: "financial institution" defined in 31 USC 5312,[3] must be at least partly located in the U.S. [(d)].	Request: "financial records"[1] [(a)(1)]. Compel: "a customer's or entity's financial records"[1] [(a)(5)(A)].	All requests under (a)(1) require certificate of RFPA compliance under 12 USC 3403(b), and must be for purposes listed in (a)(1); request by Secret Service must be for its "protective functions" [(a)(1); (a)(1)(B), (a)(2)]. FBI certifies[2] that information is sought for "foreign counter intelligence purposes to protect against international terrorism or clandestine intelligence activities," with first amendment limit[4] [(a)(5)(A)].	Dissemination by FBI allowed only as provided in AG-approved NSI Guidelines, and to another federal agency only if information "clearly relevant" to its authorized responsibilities [(a)(5)(B)].	AG must "fully inform" intelligence committees [(a)(5)(C)]. Requesting authorities must "compile an annual tabulation of the occasions in which this section was used" [(a)(4)].	Emergency access to records available in certain circumstances [(b)].
15 USC 1681u (FCRAu)	The FBI. Recipient "shall" comply[1] with request from FBI[2] [(a)-(b)].	A "consumer reporting agency" [(a)-(b)].	"names and addresses of all financial institutions … at which a consumer maintains or has maintained an account" [(a)]. "identifying information respecting a consumer, limited to name, address, former addresses, places of employment, or former places of employment" [(b)]. Note: "financial institution" defined in 12 USC 3401[5] [(a)].	FBI certifies[2] compliance with FCRAu; must first determine in writing that information is sought for conduct of "authorized investigation to protect against international terrorism or clandestine intelligence activities," with first amendment limit[4] [(a)-(b)].	Dissemination outside FBI only to other federal agencies for "a foreign counterintelligence investigation," or to the relevant military department [(f)].	AG must "fully inform" intelligence and banking committees [(h)].	FBI pays the costs of production [(e)]. Also allows court order, on FBI certification,[2] for production of a "consumer report" [(c)]. Violations trigger liquidated damages and allow injunctions, and require internal disciplinary review of responsible government employee; these remedies and sanctions are exclusive [(i), (j), (l), (m)].
15 USC 1681v (FCRAv)	A "government agency authorized to conduct investigations of, or intelligence or counterintelligence	A "consumer reporting agency" [(a)].	A "consumer report of a consumer and all other information in a consumer's file" [(a)].	Certification by a designated supervisory or Senate-confirmed officer of the agency that the information sought "is necessary" for the agency's investigation of, or	N/A	AG must "fully inform" intelligence, judiciary, house financial	

Authority	Who May Request Production?	From Whom?	Production of What?	Requirements	Dissemination	Oversight	Other
	activities or analysis related to, international terrorism" [(a)]. Recipient "shall" comply with request[1] [(a)].			intelligence or counterintelligence activities or analysis related to, international terrorism [(b)].		services, and senate banking committees [(f)].	
18 USC 2709 (ECPA)	The FBI may request[2] [(b)(1)-(2)]. Recipient "shall comply with a request … made by the Director of the Federal Bureau of Investigation under subsection (b)"[1] [(a)].	A "wire or electronic communication service provider"[6] [(a)]. Note: the term "wire or electronic communication service provider" does not include a library unless it satisfies the definition in 18 USC 2515 [(f)].	Request: "name, address, length of service, and local and long distance toll billing records" and "name. address, and length of service"[1] [(b)]. Compel: "subscriber information and toll billing records information, or electronic communication transactional records"[1] [(a)].	FBI certifies that information sought is "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities," with first amendment limit[4] [(b)].	Dissemination only pursuant to AG-approved NSI guidelines and to another federal agency if "clearly relevant" to its authorized responsibilities [(d)].	Director of FBI must "fully inform" intelligence and judiciary committees [(e)].	
50 USC 436 (National Security Act)	"Any authorized investigative agency" [(a)(1)]. Recipient "shall, if the request satisfies the requirements of this section" make records available within 30 days, except for taxpayer returns and return information under 26 USC 6103[1] [(c)(1)].	Any "financial agency, financial institution, or holding company … any consumer reporting agency" [(a)(1)].	"such financial records, other financial information, and consumer reports" [(a)(1)]. "records maintained by any commercial entity within the United States pertaining to travel by an employee in the executive branch … outside the United States" [(a)(1)].	Records pertain to current or former executive branch employee who was required to consent to access for security clearance [(a)(2)(A)]; and any one of the following: (i) "reasonable grounds" that person is or may be improperly disclosing classified information to a FP or AFP; (ii) credible evidence of excessive debt or unexplained level of affluence; or (iii) person had access and opportunity to disclose information known to have been compromised [(a)(2)(B)(i)-(iii)]. Also, financial records, other financial information, and consumer reports (not travel-related records) must be "necessary to conduct any authorized law enforcement investigation, counterintelligence inquiry, or security determination" [(a)(1)]. Certification by Assistant Secretary or higher of some of the requirements listed above in (a)(2)(A) and (a)(2)(B) [(a)(3)].	Dissemination outside the requesting agency only to employing agency, DOJ for LE or CI purposes, or to another federal agency if "clearly relevant" to its authorized responsibilities [(e)].	N/A	Requesting agency pays the costs of production [(d)].

Notes to Tab 1: Summary Table Comparing Current NSL Statutes

All NSLs contain fairly standard nondisclosure provisions. See 12 U.S.C. § 3414(a)(3)(A), (a)(5)(D); 15 U.S.C. § 1681u(d); 15 U.S.C. § 1681v(c); 18 U.S.C. § 2709(c); 50 U.S.C. § 436(b). The nondisclosure provisions provide for a certification from a designated official that, absent nondisclosure, "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." When such a certification is made, the recipient of the NSL is warned not to "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 government has sought or obtained in the information in question. The NSL must "notify the person or entity to whom the request is directed of the nondisclosure requirement." If a recipient makes an authorized disclosure (*e.g.*, to a person whose assistance is needed to comply with the request), he must "inform such persons of any applicable nondisclosure requirement," because those persons are "subject to the same prohibitions on disclosure." At the government's request, "any person making or intending to make a disclosure" must identify the person to whom the disclosure has or will be made, except for disclosure to attorneys. Nondisclosure orders are subject to challenge under 18 U.S.C. § 3511. This nondisclosure regime has been struck down as unconstitutional under the First Amendment by decision of a district court in the Southern District of New York, *Doe v. Gonzales*, 500 F. Supp. 2d 379 (2007), which at this writing is on appeal to the Second Circuit.

All NSLs also are subject to fairly standard immunity provisions. See 12 U.S.C. 3417(c); 15 U.S.C. § 1681u(k); 15 U.S.C. § 1681v(e); 18 U.S.C. § 2703(e); 50 U.S.C. § 436(c)(2).

[1]. Most NSL statutes individually require compliance with certain requests, but under 18 U.S.C. § 3511, all requests may be enforced via court order even if compliance with the request is not specified in the NSL statute itself.

[2]. References in this table to requests or certifications from the "FBI" refer to the FBI Director, or a designated FBI official at or above the level of a Deputy Assistant Director or Special Agent in Charge.

[3]. Under 31 U.S.C. § 5312(a)(2), a "financial institution" is defined to mean: (A) an insured bank (as defined in section 3(h) of the Federal Deposit Insurance Act (12 U.S.C. 1813(h))); (B) a commercial bank or trust company; (C) a private banker; (D) an agency or branch of a foreign bank in the United States; (E) any credit union; (F) a thrift institution; (G) a broker or dealer registered with the Securities and Exchange Commission under the Securities Exchange Act of 1934 (15 U.S.C. 78a et seq.); (H) a broker or dealer in securities or commodities; (I) an investment banker or investment company; (J) a currency exchange; (K) an issuer, redeemer, or cashier of travelers' checks, checks, money orders, or similar instruments; (L) an operator of a credit card system; (M) an insurance company; (N) a dealer in precious metals, stones, or jewels; (O) a pawnbroker; (P) a loan or finance company; (Q) a travel agency; (R) a licensed sender of money or any other person who engages as a business in the transmission of funds, including any person who engages as a business in an informal money

transfer system or any network of people who engage as a business in facilitating the transfer of money domestically or internationally outside of the conventional financial institutions system; (S) a telegraph company; (T) a business engaged in vehicle sales, including automobile, airplane, and boat sales; (U) persons involved in real estate closings and settlements; (V) the United States Postal Service; (W) an agency of the United States Government or of a State or local government carrying out a duty or power of a business described in this paragraph; (X) a casino, gambling casino, or gaming establishment with an annual gaming revenue of more than $1,000,000 which (i) is licensed as a casino, gambling casino, or gaming establishment under the laws of any State or any political subdivision of any State; or (ii) is an Indian gaming operation conducted under or pursuant to the Indian Gaming Regulatory Act other than an operation which is limited to class I gaming (as defined in section 4(6) of such Act); (Y) any business or agency which engages in any activity which the Secretary of the Treasury determines, by regulation, to be an activity which is similar to, related to, or a substitute for any activity in which any business described in this paragraph is authorized to engage; or (Z) any other business designated by the Secretary whose cash transactions have a high degree of usefulness in criminal, tax, or regulatory matters.

Under 31 U.S.C. 5312(c)(1), the term also includes "[a]ny futures commission merchant, commodity trading advisor, or commodity pool operator registered, or required to register, under the Commodity Exchange Act."

[4]. The First Amendment limit, which applies to certain NSL statutes, requires that the records be sought in an investigation, "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." In 12 U.S.C. § 3414(a)(5)(A) (RFPA), there is no antecedent reference to any "investigation" by the FBI before the First Amendment limit appears, but as a practical matter NSLs are in fact issued by the FBI only in the context of investigations.

[5]. Under 12 U.S.C. § 3401(1), a "financial institution" is defined to mean "any office of a bank, savings bank, card issuer as defined in section 1602(n) of Title 15, industrial loan company, trust company, savings association, building and loan, or homestead association (including cooperative banks), credit union, or consumer finance institution, located in any State or territory of the United States, the District of Columbia, Puerto Rico, Guam, American Samoa, or the Virgin Islands."

[6]. A "wire or electronic communication service provider" is defined in part in 18 U.S.C. § 2510(15), which provides that "'electronic communication service' means any service which provides to users thereof the ability to send or receive wire or electronic communications." See *United States v. Biro*, 143 F.3d 1421, 1425 n.5 (11th Cir. 1998) ("The legislative history of the Electronic Communications Privacy Act of 1986 explains that '[e]xisting telephone companies and electronic mail companies are providers of electronic communications services.'").

* * *

Tab 2: Proposed National Security Subpoena Statute

Set forth below is a draft statute providing for national security subpoenas. It is designed to be modular, so that aspects can be added, subtracted, or changed without disturbing its basic structure. It is meant to begin, not end, the conversation about improving this area of the law.

50 U.S.C. § 1881: National Security Subpoenas

(a) Requirements for Subpoena. Notwithstanding any other law, the Attorney General, or an attorney for the government designated by the Attorney General, may require by subpoena the production of any tangible thing (including books, records, papers, documents, and other items), if –

(1) The subpoena is issued in an investigation or activity authorized under Executive Order 12333 or a successor order, or in a protective investigation or activity of the United States Secret Service under 18 U.S.C. §§ 3056 and 3056A;

(2) The investigation or activity is not conducted of or concerning a United States person solely upon the basis of activities protected by the first amendment to the Constitution of the United States;

(3) The tangible things sought by the subpoena constitute or contain –

(A) information that relates to the ability of the United States to protect against the threats specified in section 101(e)(1);

(B) foreign intelligence information as defined by section 101(e)(2) that does not concern a United States person; or

(C) Secret Service protective information, which is defined to be information that relates to the ability of the United States to carry out the protective functions specified in 18 U.S.C. §§ 3056 and 3056A;

(4) The tangible things sought by the subpoena could be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation;

(5) The subpoena describes the tangible things that are to be produced with sufficient particularity to permit them to be fairly identified;

(6) The subpoena identifies the date and place at which the tangible things must be produced, which shall allow a reasonable period of time within which the things can be assembled and made available and be no more than 500 miles from the place at which the subpoena was served; and

(7) The subpoena provides clear and conspicuous notice of the principles and procedures described in subsections (c) and (d).

(b) Service of Subpoena. A subpoena issued under this section may be served by any person designated in the subpoena to serve it. Service upon a natural person may be made by personal delivery of the subpoena to him. Service may be made upon a domestic or foreign corporation or upon a partnership or other unincorporated association which is subject to suit under a common name, by delivering the subpoena to an officer, to a managing or general agent, or to any other agent authorized by appointment or by law to receive service of process. The affidavit of the person serving the subpoena entered on a true copy thereof by the person serving it shall be proof of service.

(c) Nondisclosure Requirement: Scope. If a designated official determines in writing before service of a subpoena that nondisclosure is necessary to avoid endangering the national security of the United States, interfering with a criminal, counterterrorism, or counterintelligence investigation, interfering with diplomatic relations, or endangering the life or physical safety of any person –

(1) No person shall disclose to any other person any information concerning the subpoena other than to –

(A) those persons to whom disclosure is necessary to comply with the subpoena;

(B) an attorney to obtain legal advice or assistance with respect to the production of things in response to the subpoena; or

(C) other persons as permitted by the Attorney General or an attorney for the government designated by the Attorney General.

(2) Any person to whom disclosure is made pursuant to subsection (c)(1) shall be subject to the nondisclosure requirements described in that subsection.

(3) Any person who discloses information concerning the subpoena to a person described in subsection (c)(1) shall notify such person of the nondisclosure requirements of this subsection.

(4) At the request of the Attorney General or an attorney for the government designated by the Attorney General, any person making or intending to make a disclosure under subsection (c)(1) shall identify 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 identify an attorney to whom disclosure was made to obtain legal advice or legal assistance with respect to the subpoena.

(5) For purposes of this subsection, a designated official is the Attorney General, an attorney for the government designated by the Attorney General, the head of any executive department listed in 5 U.S.C. § 101 that contains an organization listed in or designated pursuant to 50 U.S.C. § 401a(4), or any official within such an organization

designated by the department head who has been nominated by the President and confirmed by the Senate or is at or above the level of Assistant Secretary or Special Agent in Charge.

(d) Nondisclosure Requirement: Challenge and Duration. A person subject to a nondisclosure obligation under subsection (c) may at any time file a request pursuant to subsection (f) to alter the scope or duration of the obligation. In the absence of a contrary judicial order, the obligation shall remain in effect unless at any time a person subject to it provides a written objection to the attorney who issued the subpoena (or a successor attorney), and confirms receipt of that written objection by the attorney. Sixty days after receipt of the objection is confirmed, in the absence of a contrary judicial order, the obligation shall expire as to the person who made the objection.

(e) Judicial Proceedings: In General. All judicial proceedings under this section shall be concluded as expeditiously as possible. The record of proceedings, including pleadings filed, orders granted, and statements of reasons for decision, shall be maintained under security measures established by the Chief Justice of the United States, in consultation with the Attorney General and the Director of National Intelligence.

(f) Judicial Proceedings: In the FISC. The pool established by section 103(e) shall –

(1) have jurisdiction –

(A) if requested by the Attorney General or an attorney for the government designated by the Attorney General, or by any person subject to a nondisclosure obligation, to alter the scope or duration of the obligation as reasonably necessary to avoid endangering the national security of the United States, interfering with a criminal, counterterrorism, or counterintelligence investigation, interfering with diplomatic relations, or endangering the life or physical safety of any person;

(B) if requested by the Attorney General or an attorney for the government designated by the Attorney General, to issue an order requiring compliance with a subpoena, with any failure to obey the order subject to punishment as a contempt of court, and any process under this subsection allowed to be served in any judicial district in which the person or entity subject to the subpoena may be found; and

(C) if requested by the recipient of a subpoena, to quash or modify the subpoena to the extent that it is unduly burdensome or oppressive, or otherwise unlawful.

(2) within 60 days after enactment of this subsection, adopt and, consistent the protection of national security, publish procedures governing the proceedings described in subsection (f)(1). Such procedures shall –

(A) require notice and an opportunity to be heard be provided to the Attorney General or an attorney for the government designated by the Attorney General, or to the recipient of a subpoena and any other person subject to a nondisclosure obligation, as the case may be, who is not making the request;

(B) require all proceedings to be conducted in camera, and all pleadings to be filed under seal, subject to any constitutional right to an open hearing in a contempt proceeding;

(C) permit the government to file classified affidavits or other classified material ex parte; and

(D) require the judge deciding the proceeding to issue a written statement of reasons for his decision.

(g) Judicial Proceedings: Appellate Review. A party to a proceeding under subsection (f) may file a petition with the Court of Review established under section 103(b) for review of the decision issued in the proceeding not later than 7 days after the issuance of such decision. The Court of Review shall have jurisdiction to consider such petitions and shall provide for the record a written statement of the reasons for its decision. On petition for a writ of certiorari by any party to a proceeding in the Court of Review, the record shall be transmitted under seal to the Supreme Court, which shall have jurisdiction to review such decision.

(h) Immunity. Notwithstanding any Federal, State, or local law, any person, including officers, agents, and employees, receiving a subpoena under this section, who complies in good faith with the subpoena and thus produces the tangible things sought, shall not be liable in any court of any State or the United States to any customer or other person for such production or for nondisclosure of that production to the customer.

(i) Minimization Procedures.

(1) Not later than 60 days after the effective date of this section, the Attorney General shall adopt specific minimization procedures governing the acquisition, retention and dissemination of any tangible things, or information therein, sought by or received in response to a subpoena under this section. Copies of the minimization procedures shall be provided to the courts established under section 103(a) and (b), and to the Congressional committees listed in subsection (k).

(2) In this section, the term “minimization procedures” means –

(A) specific procedures that are reasonably designed in light of the purpose and technique of the particular subpoena, 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 the information described in subsection (a)(3);

(B) procedures that require that nonpublicly available information, which is not information described in subsections (a)(3)(A) or (C), 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 information described in subsection (a)(3)(B) or assess its importance; and

(C) notwithstanding subparagraphs (A) and (B) of this subsection, 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.

(j) Use of Information. Information acquired from tangible things received in response to a subpoena under this section concerning any United States person may be used and disclosed by Federal officers and employees without the consent of the United States person only in accordance with the minimization procedures adopted pursuant to subsection (i). No otherwise privileged information acquired from tangible things received in accordance with the provisions of this section shall lose its privileged character. No information acquired from tangible things received in response to a subpoena under this title may be used or disclosed by Federal officers or employees except for lawful purposes.

(k) Oversight. On a semiannual basis, the Attorney General shall fully inform the Permanent Select Committee on Intelligence and the Committee on the Judiciary of the House of Representatives, and the Select Committee on Intelligence and the Committee on the Judiciary of the Senate, concerning all subpoenas issued under this section. In addition, with respect to any subpoena served on a consumer reporting agency as defined in the Fair Credit Reporting Act, on a semiannual basis, the Attorney General shall fully inform the Committee on Financial Services of the House of Representatives, and the Committee on Banking, Housing and Urban Affairs of the Senate. The Attorney General may require any other officer of the United States to provide information to him as may be necessary to fulfill his obligations under this subparagraph.

(*l*) Audit. For three years following the effective date of this section, the Inspector General of the Department of Justice shall perform an annual audit of the effectiveness and use, including any improper or illegal use, of the investigative authority provided under this section, and shall provide a report of that audit to the Congressional committees described in subsection (k). Not less than 30 days before the submission of a report, the Inspector General shall provide such report to the Attorney General and the Director of National Intelligence, who may provide comments to be included in the report as the Attorney General or the Director of National Intelligence may consider necessary. The reports and any comments shall be in unclassified form, but may include a classified annex.